AGENCIA DE DESARROLLO RURAL – ADR

Oficina de Control Interno

N° INFORME: OCI-2020-030

DENOMINACIÓN DEL TRABAJO: Auditoría Interna a la Seguridad de la Información del Aplicativo "Banco de Proyectos".

DESTINATARIOS:[1]

- Ana Cristina Moreno Palacios, Presidente.
- Víctor Manuel Mondragón Maca, Jefe de la Oficina de Tecnologías de la Información (Delegado del Presidente - Comité de Coordinación del Sistema de Control Interno).
- César Augusto Castaño Jaramillo, Secretario General.
- Dinorah Patricia Abadía Murillo, Vicepresidente de Proyectos.
- Felipe Enrique Guerra Olivella, Jefe de la Oficina de Planeación.
- John Fredy Toro González, Vicepresidente de Gestión Contractual.
- Eduardo Carlos Gutiérrez Noguera, Vicepresidente de Integración Productiva.

EMITIDO POR: Héctor Fabio Rodríguez Devia, Jefe Oficina de Control Interno.

AUDITOR (ES): Luz Paulina Nieto Olarte, Contratista.

[1] Decreto 1083 de 2015 Artículo 2.2.21.4.7, Parágrafo 1° (modificado mediante el Artículo 1 del Decreto 338 de 2019) *"Los informes de auditoría, seguimientos y evaluaciones* [emitidos por la Oficina de Control Interno] *tendrán como destinatario principal el representante legal de la Entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva (…)"*

OBJETIVO(S): Evaluar de forma independiente el diseño y la eficacia operativa de los controles internos implementados en la Agencia de Desarrollo Rural (ADR) para gestionar los riesgos relacionados con la seguridad de la información del aplicativo “Banco de Proyectos”.

ALCANCE: El alcance establecido para la realización de este trabajo comprendió la evaluación de los controles de seguridad de la información implementados por la Agencia de Desarrollo Rural - ADR en el ciclo de procesamiento de datos en el aplicativo "Banco de Proyectos", incluyendo lo relacionado con:

- Definición, implementación y divulgación de políticas de seguridad de la información que permitan la administración y operación tecnológica del Banco de Proyectos para el registro y gestión de Proyectos Integrales de Desarrollo Agropecuario y Rural - PIDAR.
- Procedimientos de administración de la infraestructura tecnológica que soporta la operación del Banco de Proyectos
- Inventario y clasificación de activos conforme lo indican las leyes 1581 de 2012 y 1712 de 2014, el Modelo de Seguridad y Privacidad de la Información en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO 27001:2013 y demás normatividad aplicable.
- Administración de usuarios, segregación funcional y registro de eventos en el aplicativo.
- Continuidad de las operaciones en caso de pérdida intencional o involuntaria de información.
- Parametrización del aplicativo Banco de Proyectos para el registro y control de los PIDAR, conforme a los lineamientos del "Reglamento para la aprobación de los Proyectos Integrales de Desarrollo Agropecuario y Rural con Enfoque Territorial y la

Adjudicación de los Recursos que los cofinancian" (Acuerdo 007 de 2016, o en su defecto, Acuerdo 010 de 2019).

De forma transversal a la evaluación descrita, se incluyó la validación de los elementos de control referencial aplicables, relacionados en el Anexo A de la Norma Técnica ISO-IEC 27001:2013, especialmente los relacionados con: Gestión de activos, Control de acceso, Criptografía, Seguridad de las operaciones, Seguridad de las comunicaciones, Adquisición, desarrollo y mantenimiento de sistemas, Relaciones con los proveedores, Gestión de incidentes de seguridad de la información y Cumplimiento.

Período Auditado: Agosto de 2019 a Julio de 2020.

Nota: El establecimiento de este período no limitaba la facultad de la Oficina de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados.

LIMITACIONES:

Para el desarrollo de esta auditoría, el 18 de agosto de 2020 el Jefe de la Oficina de Control Interno solicitó acceso a un ambiente de pruebas del aplicativo “Banco de Proyectos”, siguiendo el procedimiento “Gestión de Solicitudes de Tecnología” (PR-GTI-002) con el diligenciamiento del formato “Solicitud de Servicios TIC” y radicado en ARANDA con TICKET-1966-1-414. Sobre el asunto, en reunión virtual vía *Microsoft Teams* del 29 de septiembre de 2020 la Oficina de Tecnologías de la Información (OTI) informó que no fue posible recrear dicho ambiente debido a fallas técnicas que no pudieron ser atendidas internamente y que requerían del apoyo del proveedor para su solución. Por lo anterior, no fue posible realizar de forma integral las pruebas de auditoría relacionadas con segregación de funciones, comprobación de las funcionalidades básicas del aplicativo, generación de reportes de excepción y registros de auditoría, así como la validación de las condiciones definidas en la parametrización del Acuerdo 007 de 2016 (a través del cual se adoptó el reglamento para la aprobación de los PIDAR con

Enfoque Territorial y la Adjudicación de los Recursos que los cofinancian) vigente para el periodo auditado y configurado en el aplicativo Banco de Proyectos. El alcance de esta prueba se extendía hasta la preparación del mismo ambiente de pruebas, así como de los datos que serían dispuestos, entre otros aspectos.

De acuerdo con lo anterior, se diseñó una prueba alterna que se desarrolló con el acompañamiento del funcionamiento del aplicativo, utilizando las cuentas de usuario genéricas que se tenían para la "migración de las iniciativas" de PIDAR que se encontraban en documentación física para ser cargadas en el aplicativo, esto, para un proyecto.

CRITERIOS: Para la realización de este trabajo se consideraron como principales criterios, los siguientes:

- Decreto 2364 de 2015 *"(...) se crea la Agencia de Desarrollo Rural - ADR, (...)"*
- Norma Técnica ISO-IEC 27001:2013. Norma que incluye todos los requisitos del *Sistema de Gestión de Seguridad de la Información*.
- Norma ISO 27002. Código de buenas prácticas para controles de seguridad de la información.
- Resolución 0409 de 2019 "*Por la cual se adopta la política de seguridad y privacidad de la información de la Agencia de Desarrollo Rural -ADR y se definen lineamientos frente al uso y manejo de la información*."
- Plan de sensibilización seguridad digital, Oficina de Tecnologías de la Información, Mayo de 2020.
- Plan de seguridad y privacidad de la información, Oficina de Tecnologías de la Información, Junio de 2020.

- Acuerdo 007 de 2016 - Artículo 18. *"(...) se adopta el reglamento para la aprobación de los Proyectos Integrales de Desarrollo Agropecuario y Rural con Enfoque Territorial y la Adjudicación de los Recursos que los cofinancian, (...)."*

- Acuerdo 010 de 2019 "*Por el cual se adopta el reglamento para los Proyectos Integrales de Desarrollo Agropecuario y Rural con Enfoque Territorial y se dictan otras disposiciones".*

- Reglamento para la aprobación de los Proyectos Integrales de Desarrollo Agropecuario y Rural con Enfoque Territorial y la Adjudicación de los Recursos que los cofinancian. (2016)

- Reglamento para Estructuración, Aprobación y Ejecución de los Proyectos Integrales de Desarrollo Agropecuario y Rural con Enfoque Territorial. (2019)

- Documentación aplicable del Sistema Integrado de Gestión - ISOLUCION *(Caracterización de proceso, procedimientos, guías, manuales, mapas de riesgos, etc.)*

- Demás normatividad aplicable.

DECLARACIÓN: Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas por la auditora a cargo de la realización del trabajo. Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

RESUMEN EJECUTIVO: Como resultado de la evaluación practicada, se identificaron oportunidades de mejoramiento relacionadas con los siguientes aspectos:

1. Falta de oportunidad en la instrumentación, formalización y aplicación de lineamientos rectores de la Política de Seguridad y Privacidad de la Información, principalmente los

relacionados con el "*Levantamiento de activos de información para seguridad digital*" para el proceso soportado por el aplicativo Banco de Proyectos, y la "*Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital*". La Política de Seguridad y Privacidad de la Información es transversal a todos los sistemas de la Entidad, por lo que es indispensable dar prioridad a la atención de los compromisos adquiridos con el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) por parte de la ADR, priorizando tareas como las antes mencionadas.

2. Inobservancia de las Políticas de Seguridad y Privacidad de la información por usuarios del aplicativo Banco de Proyectos, originada por el moderado nivel de interiorización de estas políticas por parte de los usuarios en sus actividades diarias frente al uso de los recursos informáticos y la baja participación en las capacitaciones que frente al tema que ha promovido la OTI, en coordinación con la Oficina de Comunicaciones y la Dirección de Talento Humano.

3. Incumplimiento de los lineamientos establecidos en el procedimiento de administración de usuarios y sistemas de información para la creación de cuentas en el Directorio Activo, toda vez que, en una muestra de quince (15) cuentas creadas, solo tres (3) de ellas (20%) cumplieron con los requisitos, y en las doce (12) restantes se evidenciaron desviaciones en su cumplimiento relacionadas con la documentación que se debía aportar a la OTI para su creación, evidenciándose que no se contaba con mecanismos eficaces de gestión para el almacenamiento de los soportes (requisitos), que permita la disposición organizada y oportuna de esta información, conforme lo indica la "Guía N° 6 - Gestión Documental" de MinTIC en el apartado 4 "*Normatividad Técnica Colombiana Sobre Gestión Documental*", la cual incluye tanto información física como electrónica.

4. Ausencia de lineamientos para la gestión de cuentas de usuario del Directorio Activo a nivel de Eliminación, al identificar a partir de los cruces efectuados entre los usuarios

vigentes en el Directorio Activo frente a los usuarios activos en el aplicativo Banco de Proyectos que en mayo de 2020 se realizó una depuración de 317 cuentas de usuario en el Directorio Activo, que de acuerdo con lo indicado por la OTI, fue necesario para "mejorar el rendimiento en cuanto a la búsqueda de usuarios". Al 31 de agosto de 2020 no se contaba con un procedimiento documentado y aprobado que reglamentara la eliminación de usuarios dentro del Directorio Activo y en el cual se indiquen las condiciones en las cuales se puede realizar esta actividad, así como los pasos a seguir, el responsable y la documentación soporte que se deberá generar, obtener y conservar como respaldo de las depuraciones llevadas a cabo.

5. Inadecuada gestión y monitoreo de usuarios y roles asignados en el aplicativo Banco de Proyectos, al evidenciarse 317 cuentas sin gestión en el aplicativo que correspondían a usuarios retirados de la ADR (funcionarios y/o contratistas), que si bien se habían inactivado desde el Directorio Activo, aún continuaban con rol vigente en el aplicativo Banco de Proyectos. Así mismo, se identificaron once (11) cuentas genéricas activas para Banco de Proyectos y ocho (8) cuentas con rol "Administradores", que aunque de estas últimas se conocía el responsable, no todas estaban soportadas y documentadas formalmente en cuanto a su uso.

6. Deficiencia de controles en el proceso de gestión de cambios sobre el sistema y modificaciones directas a datos en producción, en razón a que, para el período auditado no se contó con una metodología para la Gestión de Cambios Tecnológicos. Al respecto, se observó que PricewaterhouseCoopers (PwC) Asesores Gerenciales Ltda. (proveedor del aplicativo Banco de Proyectos) documentó en la versión 1 del manual del aplicativo al menos tres (3) situaciones en caso de error en el proceso, en las que se debía realizar ajustes o modificaciones sobre los datos en ambiente productivo; no obstante, la documentación de los casos en la herramienta ARANDA fue muy básica, debido a que, no se logró dar una correcta tipificación de los casos y una clara descripción de la solución. Así mismo, se conoció la realización de cambios directos a los datos en producción cuando se presentaron fallas en los formularios

XML o cuando se realizaron cargas de listas de beneficiarios a iniciativas de PIDAR cuando éstas contenían un gran número de participantes.

Por lo anterior, y considerando la documentación entregada por la OTI relacionada con los controles de cambio, no fue posible para la Oficina de Control Interno garantizar que durante el periodo evaluado no se hayan implementado otros cambios diferentes a los proporcionados por la OTI; esto sumado a que el equipo de Banco de Proyectos desconocía una funcionalidad del sistema que permitiera extraer un reporte donde se identificaran los cambios o modificaciones directas a datos en ambiente productivo para un periodo de tiempo determinado, donde se evidenciara fecha, usuario, modificación y estado del mismo.

7. Deficiencias en documentación y trazabilidad de los casos registrados en la herramienta de mesa de servicios ARANDA, relacionadas con la imposibilidad de realizar una correlación entre los incidentes creados y los soportes, la falta de un repositorio centralizado y organizado de los soportes de los incidentes atendidos que permitiera realizar una trazabilidad eficiente de todos los casos, ausencia de registro en la herramienta del detalle ordenado y suficientemente documentado del incidente reportado que facilitara identificar el riesgo, la causa del problema, el análisis de la solución y la solución aplicada (los casos se cierran con “caso cerrado” o “el requerimiento fue solucionado” sin dejar registro del resultado y afectación de la solución), así como los soportes suministrados o generados o lugar de almacenamiento de éstos. Además, no se identificó a nivel de mesa de ayuda ARANDA una métrica más allá del promedio de tiempo requerido para la atención, que le permitiera a la OTI determinar el número y gravedad del incidente atendido para realizar un análisis de los casos más críticos con los soportes de solución y así poder determinar si este era repetitivo o aislado, y poder tomar las medidas pertinentes.

8. Ausencia de procedimientos para la gestión de logs y registros de auditoria de actividades realizadas por los usuarios, debido a que, si bien el aplicativo Banco de Proyectos cuenta con una serie de logs activos de autoría predefinidos, no fue posible determinar las acciones y actividades que registraba, evidenciando que la administración del sistema no tenía un claro conocimiento de la información que se generaba como rastro de auditoría, tanto a nivel de consulta como de la estructura e interpretación de los registros. Adicionalmente, se evidenció la ausencia de monitoreo sobre los logs que estaban activos y su responsable, como también la falta de identificación de informes de errores y excepciones, y definición de las actividades críticas que debían ser monitoreadas en el sistema.

9. Inadecuada gestión y monitoreo de mecanismos de recuperación en caso de contingencia, al observar que si bien se generaban copias de respaldo con una frecuencia diaria, en una muestra de 40 fechas de copias de respaldo para base de datos del aplicativo y los servidores, solo se obtuvo evidencia del 25% de la documentación requerida en el procedimiento Generación y Administración de copias de seguridad de las Bases de Datos. En cuanto a las pruebas de restauración, solo se obtuvo evidencia de esta actividad para el mes de agosto de 2019. Así mismo, se identificó que el proveedor PwC proporcionó el documento “Plan de Contingencia - Banco de Proyectos” con fecha 31 de octubre de 2017 del cual no se realizaron pruebas para el aplicativo, ni antes ni posterior a la puesta en producción de la versión 2, y de la migración de los servidores a la nube. Al 30 de septiembre de 2020 se desconocía la aplicabilidad y vigencia del documento proporcionado por el proveedor.

10. Ausencia de lineamientos para el monitoreo de capacidad y disponibilidad de la infraestructura tecnológica hardware y software para Banco de Proyectos, en razón a que, al 31 de julio de 2020 la ADR no contaba con un procedimiento formalizado y divulgado para la gestión de la capacidad y disponibilidad de los servidores y las bases de datos, que le permita a la OTI soportar las actividades de monitoreo que ejecuta y tomar decisiones con base en estadísticas y tendencias de detección para la

implementación de mejoras en el desempeño de bases de datos, sistemas operativos y software de aplicación.

11. Inobservancia del desarrollo de pruebas de vulnerabilidad al Banco de Proyectos y su entorno, teniendo en cuenta que, aunque en el escaneo realizado al aplicativo Banco de Proyectos en abril de 2020 se identificaron alertas y posibles soluciones proporcionadas por la herramienta con la que se ejecutó el escaneo, no se contó con un análisis técnico por parte del ejecutor del control, que le permitiera a la ADR establecer los impactos internos e identificar falsos positivos; además, la actividad realizada estaba incompleta y no cumplió con el objetivo que propone un ejercicio de pruebas de vulnerabilidad, como tampoco incluyó la gestión de las vulnerabilidades identificadas, mediante la generación de un plan de acción y la mitigación de riesgos.

    Adicionalmente, durante el período auditado no se evidenció la realizaron de pruebas de seguridad perimetral, las cuales son necesarias, toda vez que, el aplicativo Banco de Proyectos se encuentra público en internet, y para su acceso se dispone de dispositivos que apoyan su seguridad y restricción de acceso que deben ser evaluados periódicamente.

RIESGOS IDENTIFICADOS EN LA AUDITORÍA:

Incluidos en el Mapa de Riesgos de Gestión

DESCRIPCIÓN	CUBIERTO EN LA AUDITORIA
Proceso Evaluación, Calificación y Cofinanciación de Proyectos Integrales (CP-ECC-001)	
Falla en la operatividad en el aplicativo Banco de Proyecto, para el módulo de Proyectos, Evaluación y Calificación.	Si

Incluidos en el Mapa de Riesgos de Corrupción

DESCRIPCIÓN	CUBIERTO EN LA AUDITORIA
Proceso Evaluación, Calificación y Cofinanciación de Proyectos Integrales (CP-ECC-001)	
Calificación y evaluación de proyectos por parte de los servidores de la ADR no ajustados a los criterios definidos para favorecimiento con recursos públicos a un tercero o para beneficio propio.	Si
Proceso Gestión de Tecnologías de la Información (CP-GTI-001)	
Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero.	Si

Identificados por la Oficina de Control Interno *(en su evaluación preliminar y durante la ejecución de la auditoría)**:***

DESCRIPCIÓN	CUBIERTO EN LA AUDITORIA
Fuga de información a causa de accesos no autorizados al sistema.	Si
Incumplimiento legal de normas/leyes internas y externas aplicables a los procesos de ADR.	Si
Fallas tecnológicas en el aplicativo Banco de Proyectos y/o en la infraestructura técnica (hardware, redes y comunicaciones) que lo soporta, que afecta la seguridad de la información.	Si
Acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos.	Si
Errores en la ejecución de procesos que impidan la disponibilidad de la información.	Si
Dependencia del conocimiento del Profesional que ejecuta el control, por ausencia de documentación necesaria para su desarrollo y gestión.	Si
Falla humana en la ejecución de los procesos al desconocer u omitir los lineamientos de seguridad implementados por la ADR, que deriven en pérdida de seguridad y privacidad de la información.	SI

AVANCE DEL PLAN DE MEJORAMIENTO VIGENTE AL INICIO DE LA AUDITORÍA:

Teniendo en cuenta el enfoque de esta auditoría, durante su ejecución se realizó seguimiento al hallazgo "*Omisión de logs de auditoría e informes de errores y excepciones de la operatividad del aplicativo Banco de Proyectos y del ambiente de pruebas de la herramienta*" identificado por la Oficina de Control Interno en la Auditoría Interna Especial al Aplicativo Banco de Proyectos realizada en la vigencia 2019 y registrado en el informe OCI-2019-017; hallazgo que no fue aceptado por los responsables de la unidad auditada, sobre lo cual, la Oficina de Control Interno conceptuó y comunicó lo siguiente:

"*Una vez analizada la respuesta remitida por los responsables de la actividad auditada, esta Oficina de Control Interno no la encuentra razonable, dado que no argumenta el punto crítico del hallazgo, esto es, el seguimiento y monitoreo que debe efectuar la Agencia de Desarrollo Rural a los logs de auditoría y a las excepciones derivadas de los informes de errores y excepciones que produce el aplicativo Banco de Proyectos.*

Además, (…) la Oficina de Tecnologías de la Información (OTI), (…) indicó que el archivo de logs de las funcionalidades del Banco de Proyectos no estaba siendo monitoreado por ellos, por lo que se concluyó que la Entidad no está realizando ni la generación ni el seguimiento esperado de dichos registros. Igual situación sucede con los informes de errores y excepciones, que, si bien pueden ser generados por la herramienta, no fueron entregados ni tampoco se evidenció su seguimiento por un servidor público de la Entidad.

Respecto al ambiente de pruebas, aunque no es un entregable del contrato, esta herramienta se analizó como un elemento importante para realizar desarrollos nuevos y verificar el funcionamiento de la herramienta a través de la ejecución de pruebas de validación de alertas que genere el aplicativo. La inexistencia de este ambiente de pruebas fue motivo para que esta Oficina de Control Interno no pudiera cerciorarse de la validez de los registros y alertas generadas por el aplicativo Banco de Proyectos.

Por lo anterior, la Oficina de Control Interno recomienda que se establezcan acciones de mejoramiento para subsanar las situaciones descritas e identificadas en este hallazgo y que no fueron aceptadas por los responsables de la actividad auditada, para que los riesgos identificados y asociados a este hallazgo sean gestionados o mitigados; en consecuencia, se mantienen las situaciones observadas por esta Oficina de Control Interno, por lo que este hallazgo continuará abierto hasta que se identifiquen las causas que lo generaron, y se formulen y ejecuten las acciones necesarias que lo subsanen."

En el proceso de seguimiento, la Oficina de Control Interno observó que, si bien el aplicativo Banco de Proyectos cuenta con una serie de logs de autoría predefinidos y activos, a 31 de agosto de 2020 no se habían tomado acciones encaminadas a la apropiación, monitoreo y análisis de los registros de auditoría por parte del equipo asignado al Banco de Proyectos, del cual hacen parte dos (2) personas de la Oficina de Tecnologías de la Información y el líder funcional de la Vicepresidencia de Proyectos; situación que se reporta detalladamente en el hallazgo N° 8 del presente informe.

En cuanto al ambiente de pruebas, se mantiene la observación reportada en el informe del año 2019, teniendo en cuenta la limitación en el alcance presentada en esta auditoría y reportada en este informe, al no poder verificar, entre otros, el funcionamiento de la herramienta a través de la ejecución de pruebas de validación de alertas que pueda generar el aplicativo.

HALLAZGOS:

NOTA: *La información detallada de las situaciones que se describen a continuación, se suministró en cada reporte de hallazgo (formato F-EVI-013) al personal designado para atender la auditoría y fue suscrito por los responsables de la Unidad Auditada y por la Oficina de Control Interno; además, dicho detalle se encuentra registrado en los papeles de trabajo elaborados por la auditora que practicó las pruebas, los cuales son custodiados por la Oficina de Control Interno; no obstante, estos documentos se encuentran*

disponibles para consulta de las partes interesadas, previa solicitud formal de los mismos al Jefe de la Oficina de Control Interno.

HALLAZGO N° 1. Falta de oportunidad en la instrumentación, formalización y aplicación de lineamientos rectores de la Política de Seguridad y Privacidad de la Información.

Descripción: La Agencia de Desarrollo Rural (ADR) ha basado su modelo de seguridad de la información en el modelo propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). En virtud de la adopción de la "Política de Seguridad y Privacidad de la Información" a través de la Resolución 0409 el 3 de julio de 2019 y del "Plan de Seguridad y Privacidad de la Información" propuesto por la ADR para dar cumplimiento con los requerimientos del "Modelo de Seguridad y Privacidad de la Información "(MSPI), la Oficina de Control Interno realizó seguimiento al nivel de avance e implementación de los compromisos establecidos en el Plan de Seguridad y Privacidad de la Información - sección 12. Cronograma, relacionados con políticas transversales de seguridad informática que resultan atribuibles al aplicativo Banco de Proyectos, en lo que se observó que se ha venido trabajando en las tareas planteadas, y que si bien la Oficina de Tecnologías de la Información (OTI) contaba con un responsable para la coordinación y ejecución del plan, se identificaron desfases en la ejecución de las siguientes tareas programadas, situación que podría derivar en un posible incumplimiento de los compromisos adquiridos con MinTIC, y en la oportunidad en la aplicación de lineamientos de Seguridad y Privacidad de la Información en la ADR.

COMPROMISO – GESTIÓN	FECHA FINAL	OBSERVACIÓN
GESTIÓN DE ACTIVOS		
Levantamiento de activos de información para seguridad digital	30-ago-2020	Vencida. Al 11-sep-2020 los ingenieros de la OTI se encontraban realizando el levantamiento de la información con las áreas de la ADR, mediante la aplicación del instrumento diseñado para este fin. Esta actividad se documenta en el formato "Registro de Activos de Información de Seguridad Digital" (F-GTI-010). Al 25-sep-2020, lo

COMPROMISO – GESTIÓN	FECHA FINAL	OBSERVACIÓN
		pertinente al proceso soportado por el Banco de Proyectos aún no se encontraba disponible. El Instructivo "Desarrollo de inventario y clasificación de activos de información" (IN-GTI-001) - versión 2, define la metodología, la cual lista 6 pasos para el desarrollo del inventario, de los cuales, a la entrega de todos los formatos de "Registro de Activos de Información de Seguridad Digital" se estaría dando cubrimiento a los pasos: 1. Listar los activos por proceso, 2. Identificar el dueño de los activos, 3. Clasificar los activos, y 4. Clasificar la información (conforme a las leyes y normativas aplicables), quedando por realizar los pasos críticos del levantamiento de los activos de información, siendo los de mayor análisis y complejidad por el criterio que se requiere, como se describe a continuación. ▪ *Paso 5. Determinar la criticidad del activo.* Queda por cerrar lo concerniente a que "*la ADR debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentando y aprobado por la Línea Estratégica - Alta dirección*". ▪ *Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas - ICC.* Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios: 1) 250.000 personas (Impacto Social), 2) $464.619.736 (Impacto Económico), o 3) Tres años en recuperación (Impacto Ambiental).
GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL		
Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital.	30-ago-2020	Vencida. El atraso en la actividad "Levantamiento de activos de información para seguridad digital", impacta directamente la tarea "Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información".
PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN		
Documento para ingreso seguro a los sistemas de información Crear documento de gestión de usuarios y contraseñas	31-jul-2020	Vencida. Se tienen lineamientos base para el desarrollo de estos tres (3) documentos fundamentales para la gestión de usuarios propendiendo la salvaguarda de la información en el sistema, desde el acceso lógico.

COMPROMISO – GESTIÓN	FECHA FINAL	OBSERVACIÓN
Política de gestión de control de acceso en el manual de políticas del Modelo de Seguridad y Privacidad de la Información		
Política de criptografía en manual de políticas del Modelo de Seguridad y Privacidad de la Información	31-ago-2020	Vencida. El Profesional Especializado Seguridad Informática señaló que, con base en los análisis efectuados no se realizará una política adicional como se estimó, sino que se irá alineado al manual de políticas.
Crear documento de gestión de capacidad infraestructura	01-jun-2020	Vencida. Se observó un documento en calidad de borrador, el cual estaba en proceso de revisión por parte del Profesional Especializado Seguridad Informática, toda vez que, debe realizar ajustes acordes a la infraestructura con la que cuenta la ADR, para pasarlo a revisión del Jefe de la OTI.
Documento para el tratamiento de la seguridad en los acuerdos con los proveedores.	01-jul-2020	Vencida. Se observó un borrador del documento "Confidencialidad proveedores ADR" para revisión del Jefe de la OTI. Una vez se cuente con su aprobación, se pasará a la Vicepresidencia de Gestión Contractual para su revisión y aprobación y, posterior publicación.
Revisar documento adquisición, desarrollo y mantenimiento de software	01-jul-2020	Vencida. Se observó un borrador del documento "Confidencialidad proveedores ADR" para revisión del Jefe de la OTI.
SEGURIDAD EN LA NUBE		
Aseguramiento de la información en la nube	30-jun-2020	Vencida. De acuerdo con lo informado por el Profesional Especializado Seguridad Informática, la ADR se acogió al lineamiento de MinTIC para subcontratar. Al respecto, la "*Guía N° 12 - Seguridad en la Nube"* de MinTIC, en el apartado 9.2.1 "*Subcontratación*" señala que: *"Las obligaciones del proveedor en materia de seguridad se transmiten de forma transitiva a las partes subcontratadas. En particular los niveles de seguridad de la información a la que tenga acceso el proveedor, y de los servicios que de este último dependan. La parte subcontratada deberá atender a los requisitos de seguridad derivados*". Al respecto, la Oficina de Control Interno señaló que, si bien existe una transferencia del control a un tercero, es responsabilidad de la ADR velar por el cumplimiento del monitoreo y seguimiento como ente contratante. Es así,

COMPROMISO – GESTIÓN	FECHA FINAL	OBSERVACIÓN
		como la misma Guía N° 12, en el apartado 7. 1 "*Características Esenciales*", cita: "[…]. *Hay que mencionar que, si la entidad lleva sus servicios a la Nube, tercerizando diferentes tareas de gestión de TI; nunca debe perder el control sobre la información y sobre la seguridad. Antes de contratar este tipo de servicios es primordial evaluar las condiciones del servicio y las medidas de seguridad aplicadas; es decir, que las condiciones sean las adecuadas para garantizar el servicio y la protección de la información de la entidad.*" (subrayado fuera de texto)

Dentro de los compromisos establecidos y sujetos a esta revisión, se observaron cumplidos los siguientes, aunque por fuera de la fecha final establecida para su cumplimiento:

COMPROMISO – GESTIÓN	FECHA FINAL ESTABLECIDA	FECHA DE CUMPLIMIENTO	PRODUCTO / RESULTADO
Gestión de Incidentes de Seguridad de Información Publicar y socializar el procedimiento actualizado de incidentes de seguridad de la información.	15-dic-2019	18-jun-2020	Procedimiento "Gestión de Incidentes de Seguridad de la Información" (PR-GTI-004) Versión 2, publicado en ISOLUCIÓN el 18-jun-2020. Formato "Reporte de Gestión de Incidente o Evento de Seguridad" (F-GTI-009) Versión 1, publicado en ISOLUCIÓN el 18-jun-2020.
Procedimiento Seguridad de la Información Documento de protección contra códigos maliciosos.	01-jun-2020	09-sep-2020	Instructivo "Gestión de Código Malicioso" (IN-GTI-003) Versión 1, publicado en ISOLUCIÓN el 9-sep-2020.

Adicionalmente, en la revisión del cumplimiento del compromiso "Definir lineamientos para ejecutar las pruebas de vulnerabilidades" que tenía fecha de finalización el 31 de agosto de 2020, considerando los requisitos establecidos en la "Guía Metodológica de Pruebas de Efectividad" del MinTIC, numeral 10 "Pruebas y Análisis" y sus secciones subsecuentes, no se observaron avances.

De otra parte, teniendo en cuenta que, en el Artículo Décimo Noveno de la Resolución 0409 de 2019 se estableció: "*La Política de Seguridad y Privacidad de la Información, será revisada anualmente, o antes si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz. Este proceso será liderado por el Oficial de Seguridad de la Información o quien haga sus veces*", y que ésta entró en vigencia el 3 de julio de 2019, fecha en la cual fue puesta en conocimiento público de funcionarios y contratistas de la ADR, se validó este aspecto con el Profesional Especializado Seguridad Informática evidenciando que, si bien la Agencia de Desarrollo Rural - ADR se encontraba en proceso de diseño e implementación de los diferentes lineamientos del Plan de Seguridad y Privacidad de la Información conforme lo ha establecido en la sección 12 del mismo, la Oficina de Control Interno no identificó que al 31 de agosto de 2020 se hubiera realizado revisión y actualización puntual de la política mencionada.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Insuficiencia de recurso humano en la Oficina de Tecnologías de la Información a raíz de restricciones presupuestales o requerimientos de perfiles específicos que dificultan la asignación y distribución de las labores de Seguridad de la Información. ▪ Estado de madurez del Modelo de Seguridad y Privacidad de la ADR en proceso de fortalecimiento. ▪ Concentración de tareas en el Profesional Especializado Seguridad Informática.	▪ Incumplimiento legal de normas/leyes internas y externas aplicables a los procesos de ADR. ▪ Dependencia del conocimiento del Profesional Especializado Seguridad Informática del Modelo de Seguridad de la ADR, por ausencia de documentación necesaria para su operación y gestión.	▪ Multas o sanciones de entes reguladores por incumplimiento de los compromisos. ▪ Fuga o robo de información, acceso abierto a datos o a información reservada, confidencial o restringida por usuarios no autorizados. ▪ Violación de leyes de derechos de autor o de habeas data. ▪ Aplicar discrecionalmente criterios no aprobados por el ente facultado. ▪ Pérdida de confidencialidad en el tratamiento de los datos personales de los usuarios de los PIDAR a través del Banco de Proyectos, por no contar con un inventario de activos digitales (información física/electrónica que almacenan datos personales) valorado y gestionado.

Recomendación(es):

Teniendo en cuenta que las políticas de seguridad y privacidad de la información son transversales a todos los sistemas de la Entidad, y que el Profesional Especializado

Seguridad Informática lleva un control minucioso del avance de cada actividad, se hace indispensable contar con los recursos necesarios y el tiempo para atender los compromisos adquiridos, priorizando las tareas que requieren mayor esfuerzo y mayor responsabilidad, como corresponde al levantamiento de activos de información para seguridad digital, así como la tarea subsiguiente, "Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital".

En el documento para el tratamiento de la seguridad de la información en los acuerdos con los proveedores, se recomienda considerar los siguientes aspectos:

- Con base en la metodología definida por la ADR, en el Instructivo "Desarrollo de inventario y clasificación de activos de información" (IN-GTI-001) Versión 2, realizar la identificación de los activos de información relacionados con las actividades que desarrollará el proveedor. Es importante precisar que, si se trata de un proveedor que asume a largo plazo el manejo y operación de una o más funciones clave de la entidad, o en un servicio suministrado con un activo que almacene o procese información se deberá realizar el análisis de riesgos de seguridad de la información.

- Teniendo en cuenta la valoración resultante en la clasificación en cuanto a la Confidencialidad, Integridad y Disponibilidad de los activos de información, se podrán definir los requerimientos de protección a incluir en los procesos de selección del proveedor.

- Así mismo, debe ser considerado si los activos de información almacenan o procesan datos personales para asegurar el cumplimiento de la Ley 1581 de 2012.

Para el documento "Aseguramiento de la información en la nube": realizar la elaboración del documento, teniendo en cuenta que es responsabilidad de ADR, velar por el cumplimiento del monitoreo y seguimiento como ente contratante, y que como se cita en la Guía N° 12 del MinTIC, […] "*nunca debe perder el control sobre la información y sobre la seguridad*". Antes de contratar este tipo de servicios es primordial evaluar las

condiciones del servicio y las medidas de seguridad aplicadas; es decir, que las condiciones sean las adecuadas para garantizar el servicio y la protección de la información de la entidad. Si bien Azure cuenta con la certificación ISAE por sus siglas en inglés -International Standard on Assurance Engagements, dependiendo del producto/servicio en los reportes SOC - Service Organization Controls SOC 1, SOC 2 y SOC 3, los cuales puede descargar desde la página de Microsoft[2], es importante que la OTI realice anualmente la revisión de estas evaluaciones, con el fin de que se asegure que cumple con los deberes que Microsoft le transfiere, como por ejemplo, actualización de parches que están a cargo de los contratantes.

Respuesta del Auditado: Aceptado Parcialmente

Justificación: "*Teniendo en cuenta la observación realizada en la reunión de apertura de considerar los planes propuestos con anterioridad por la Oficina de Tecnologías de la información en relación al siguiente propuesto "Revisar, actualizar y/o definir los procesos de la OTI, conforme lo establecido en el Plan Estratégico de Tecnologías de la Información aprobado por el Comité Institucional de Gestión y Desempeño del 20 de diciembre de 2019, y de acuerdo con las modificaciones en el mapa de procesos de la ADR aprobadas en el Comité Institucional de Gestión y Desempeño del 17 de julio de 2020, que comprende la inclusión del proceso de apoyo "Operación de los servicios tecnológicos" y cambio de nombre del proceso "Gestión de Tecnologías de la Información" por "Estrategia de Tecnologías de la Información". Adicionalmente, este ejercicio comprende la actualización y/o modificación del proceso y procedimientos que se encuentran formalizados en ISOLUCION y la definición del nuevo proceso y sus procedimientos vinculados. En ese sentido, las actividades relacionadas con la actualización, modificación y/o definición de procesos procedimientos de la OTI se tiene definido realizar en la vigencia 2020 hasta el mes de diciembre." Del cual, en fecha de entrega esta para el 31 de diciembre de 2020, es de aclarar que, los documentos*

[2] https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide

mencionados en el Hallazgo están incluidos en esta mejora (…) y dado el alcance de la auditoria (…), se relacionan evidencias en justificación a los siguientes puntos:

1. ***SEGURIDAD EN LA NUBE**. Esta actividad no está vencida dado que como se mencionó, la "Guía N° 12 - Seguridad en la Nube" de MinTIC, en el apartado 9.2.1 "Subcontratación" señala que: "Las obligaciones del proveedor en materia de seguridad se transmiten de forma transitiva a las partes subcontratadas. En particular los niveles de seguridad de la información a la que tenga acceso el proveedor, y de los servicios que de este último dependan. La parte subcontratada deberá atender a los requisitos de seguridad derivados". Para lo cual, la Entidad cuenta con un contrato vigente y desde el año 2017 cuando decidió adquirir los servicios en la nube y realizó el estudio para seleccionar el operador y validar que se cumplieran los lineamientos de seguridad, por esta razón, desde ese momento se cuenta con este proveedor de nube, y los años siguientes lo que se ha realizado es renovación o recompra de créditos para su uso. Adicional a esto, los contratos celebrados desde Colombia Compra Eficiente cuentan con un Acuerdo Marco donde están descritas las condiciones de servicio:*

   - *En el Acuerdo Marco de nube pública III CCENEG-015-1-2019, en la sección de descargas se encuentra el "Anexo 1 - Condiciones Transversales" y en la hoja nombrada "Condiciones Transversales" se encuentra el apartado de Gestión de Seguridad donde se especifican los lineamientos de seguridad que debe cumplir el proveedor de servicios. https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/nube-publica-iii*

   - *Los anteriores lineamientos definidos en el Acuerdo Marco, los cumple el proveedor Microsoft a través de su portal de Azure y se puede encontrar todo lo respectivo al tema de seguridad en la página de Microsoft. https://docs.microsoft.com/es-mx/azure/architecture/framework/security/overview*

En relación a la observación "nunca debe perder el control sobre la información y sobre la seguridad", la Oficina de Tecnologías de la Información cuenta con la contratación de un profesional especializado administrador de infraestructura tecnológica quien está a cargo de la administración de los créditos en AZURE, así como de realizar la verificación del contrato vigente. Dado lo anterior, no se acepta este hallazgo ya que para la OTI la seguridad en la nube está controlada.

2. ***PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN.*** *Se entiende que el cumplimiento del plan es importante dado que se alinea al cumplimiento del MSPI en la ADR, pero como se especificó, la Oficina de Tecnologías de la información está en la actualización de sus procesos, y en el plan de mejora vigente está con fecha hasta el 31 de diciembre de 2020, y se están elaborado los documentos mencionados en esta actualización, por lo cual, se relacionan unos documentos que no dan para el alcance de esta auditoria y se relaciona la siguiente justificación:*

   - *Crear documento de gestión de usuarios y contraseñas. La creación de este documento no afecta los controles del alcance Seguridad de la Información del Aplicativo "Banco de Proyectos", dado que el ingreso al aplicativo Banco de Proyectos se hace por el directorio activo alineado al procedimiento documentado "PR-GTI-006 Administración de usuarios y Sistemas de Información", de esta manera, no contar con el documento no afecta el control que se tiene con la creación de usuarios desde la mesa de servicio.*

   - *Política de gestión de control de acceso en el manual de políticas del Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de criptografía en manual de políticas del MSPI están dentro del manual de políticas de seguridad, el cual fue elaborado con los instrumentos enviados por MinTIC y aprobado por los mismos, y se solicitará aprobación en el próximo Comité Institucional de Gestión y Desempeño. Se adjunta correos con la aprobación y el manual, con este documento se subsanan estas políticas.*

- *Documento para el tratamiento de la seguridad en los acuerdos con los proveedores. Como se había relacionado, los acuerdos deben estar alineados a los contratos, por lo cual, se envió un memorado con número de radicado 120202400027203 y con asunto: "Documento para el tratamiento de la seguridad en los acuerdos con los proveedores" (…). Por lo cual, este hallazgo no se acepta dado que es una decisión de la Vicepresidencia de Gestión Contractual implementar los acuerdos para la ADR.*

- *Revisar documento adquisición, desarrollo y mantenimiento de software. Para este documento ya se tiene en ISOLUCION el procedimiento PR-GTI-003 Desarrollo, Implementación y Mantenimiento de Sistemas de Información (Versión 2).*

3. ***GESTIÓN DE ACTIVOS.*** *Con el fin de dar cumplimiento al MSPI se realizó el levantamiento de activos de seguridad digital mediante la actualización del documento IN-GTI-001 Desarrollo de Inventario y Clasificación de Activos de Información y la elaboración del formato F-GTI-010 Registro de Activos de Información de Seguridad Digital, esto no significa que la Entidad no contara con el levantamiento de activos de información, ya que se tiene el inventario publicado en nuestro portal WEB con corte a 2019, (…). Se cuenta con el levantamiento de activos a la fecha, pero se han tenido dificultades para realizarlo ya que algunas áreas no disponen de tiempo para asistir a las citas programada por los profesionales de la OTI. Se acepta la observación dado que, los activos faltantes corresponden a los procesos relacionados con el Banco de Proyectos y es importante contar con la criticidad de los activos. Se pretende realizar la gestión de riesgos de seguridad digital, por lo cual, se propone un plan de mejora a 31 de octubre de 2020 para completar el 100% del levantamiento de activos de seguridad digital. (…).*

4. ***GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL*** *en relación con la Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital. Se debe contar con los activos para realizar esta actividad, alineada*

a la metodología de riesgo de la ADR; sin embargo, el MinTIC envió el documento instrumento que adjuntamos para realizar los riesgos, por lo expuesto, y teniendo en cuenta que debemos contar con el análisis de riesgos de los procesos que interactúan con el Banco de Proyectos se acepta la observación y se plateará un plan de mejora a diciembre de 2020.

Con respecto al "Documento para ingreso seguro a los sistemas de información" y "Crear documento de gestión de capacidad infraestructura", aunque contamos con los instrumentos y controles (…) no se cuenta con la aprobación y publicación de estos documentos, por lo cual, se acepta realizar un plan de mejora para aprobación y publicación de estos documentos a diciembre de 2020."

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Falta de atención por parte de los responsables de los procesos en las citas programadas para terminar con el ejercicio de levantamiento de activos de seguridad digital.
- Debilidad en los controles aplicados que permitan que posibles amenazas y probables eventos no deseados puedan causar daños y consecuencias afectando la seguridad de la información.
- Debilidades por acceso no autorizado a la información mantenida por los sistemas y aplicaciones.
- Insuficientes recursos de infraestructura tecnológica que comprometan los servicios que se brindan en la entidad

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Proyectar oficios formales a los dueños de los procesos de Estructuración de Planes Integrales de Desarrollo Agropecuario y Rural, Evaluación, Calificación y Cofinanciación de Proyectos Integrales, Fortalecimiento a la Prestación del Servicio Público de Extensión Agropecuaria y de Gestión Contractual, con el fin de realizar el diligenciamiento del instrumento de F-GTI-010 Registro de Activos de Información de Seguridad Digital.	Registro de activos de información de seguridad digital del 100% de los procesos de la ADR.	Correctiva	Equipo Humano OTI	10-oct-2020	31-oct-2020
Realizar la Identificación, Análisis y Evaluación de Riesgos de Seguridad Digital con el instrumento enviado por Mintic.	Identificación, análisis y evaluación de riesgos de Seguridad Digital con instrumento enviado por MinTIC de mapa de riesgos de Seguridad de la Información.	Preventiva	Equipo Humano OTI	10-oct-2020	31-dic-2020
Realizar la elaboración del documento para ingreso seguro a los sistemas de información para gestionar el acceso a los sistemas de información de manera segura, empleando métodos preventivos contra ataques de fuerza bruta, validando los datos completos para ingreso a los sistemas.	Documento para ingreso seguro a los sistemas de información.	Correctiva	Equipo Humano OTI	10-oct-2020	31-dic-2020
Crear documento de gestión de capacidad infraestructura, gestión de la capacidad para los sistemas de información crítico. La Entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda. Aunque se cuenta con el catálogo de servidores como instrumento de monitoreo de capacidad es importante contar con el documento guía.	Documento de gestión de capacidad infraestructura.	Correctiva	Equipo Humano OTI	10-oct-2020	31-dic-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Una vez analizadas las justificaciones del equipo auditado, esta Oficina de Control Interno expone sus argumentos en el mismo orden en que fueron detallados por los auditados los asuntos de este hallazgo en la justificación, tomando como base las buenas prácticas en temas de Gobierno que propone COBIT 2019 y el "Marco de Referencia de Arquitectura Empresarial[3]" que expone el MinTIC, donde en el Dominio Gobierno de TI, señala "*Este dominio brinda directrices para implementar esquemas de gobernabilidad de TI y para adoptar las políticas que permitan alinear los procesos y planes de la institución con los del sector*", así como lo hace en el ámbito "*Esquema de Gobierno TI. Busca la agrupación de los elementos necesarios para que la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces establezca las capacidades, procesos y esquemas de gobernabilidad de TI; bajo los cuales pueda monitorear, evaluar y redirigir las TI dentro de la institución.*"

1. **SEGURIDAD EN LA NUBE.** La OTI proporcionó los estudios previos en los cuales no se señalaron controles de supervisión del contrato; además, la Oficina de Control Interno revisó los documentos disponibles para consulta en la página web de Colombia Compra Eficiente y no evidenció el contrato al que hace referencia la OTI. Es importante precisar que, esta información se solicitó al ingeniero a cargo de la Administración de Infraestructura. Ahora bien, la recomendación está encaminada a fortalecer los controles que se tengan desde la supervisión del contrato con la inclusión de la revisión de los reportes SOC (Service Organization Controls) SOC 1, SOC 2 y SOC 3 para los servicios contratados con Microsoft AZURE, los cuales señalan controles que transfiere el proveedor al cliente, en este caso a la ADR. Por otra parte, cuando se indica *"[…] cuenta con la contratación de un profesional especializado administrador de infraestructura tecnológica quien está a cargo de la administración de los créditos en AZURE, así como realizar la verificación del contrato*

[3] Fuente: https://mintic.gov.co/arquitecturati/630/w3-channel.html

vigente", la Oficina de Control Interno detalla en este hallazgo situaciones observadas en cuanto a la administración de la capacidad de la infraestructura tecnológica, razón por la cual, se hace aún más necesaria la formalización del lineamiento que detalle y direccione a otros procedimientos las actividades a realizar.

Respecto a los puntos expuestos anteriormente, la actividad se indica vencida debido a que no se observó un lineamiento que dé cumplimiento formal a la actividad propuesta en el MSPI y que se alinee con los controles de la OTI. La Oficina de Control Interno no acepta la justificación, toda vez que, se está entregando evidencia nueva que no fue suministrada en el momento de las pruebas de auditoría y ésta adolece de las mismas características de validez y suficiencia para corroborar la oportunidad de ejecución de la actividad de control.

2. **PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN:**

- Crear documento de gestión de usuarios y contraseñas. La argumentación de la OTI no es aceptada, puesto que los documentos mencionados tienen total validez para Banco de Proyectos, teniendo en cuenta que la creación de usuarios y configuración de políticas de contraseñas se realiza a través del Directorio Activo, que es donde se da inicio a la creación del usuario en la ADR.

- Se hace mención a la "*Política de gestión de control de acceso en el manual de políticas del Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de criptografía en manual de políticas del MSPI están dentro del manual de políticas de seguridad"*, para lo cual la OTI adjunta correo electrónico del jueves 24 de septiembre de 2020, lo cual corresponde a evidencia nueva y fuera del período auditado.

- Documento para el tratamiento de la seguridad en los acuerdos con los proveedores. Al igual que el punto anterior, se está entregando evidencia nueva y

fuera del periodo auditado, memorando 120202400027203 del 21 septiembre de 2020.

- Revisar documento adquisición, desarrollo y mantenimiento de software. Si bien se encuentra en ISOLUCIÓN la versión 2 del procedimiento Desarrollo, Implementación y Mantenimiento de Sistemas de Información, publicado el pasado 1 de octubre de 2020, su versión preliminar era del 12 de septiembre de 2017 y no daba cubrimiento al ciclo de vida de software de manera integral y aplicable a las condiciones actuales de la ADR y del aplicativo Banco de Proyectos; con base en lo anterior, se está entregando evidencia nueva y fuera del período auditado.

3. **GESTIÓN DE ACTIVOS:** El hallazgo está dirigido a las acciones a tomar para la actividad "Levantamiento de activos de información para seguridad digital", y no se hace mención a las actividades programada para el año 2019, las cuales no fueron seleccionadas para revisión por parte de esta Oficina de Control Interno.

   Como se indicó en la evaluación, se han adelantado gestiones, pero aún hacen falta actividades importantes para la finalización, situación que la OTI también reconoce en la justificación.

4. **GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL.** Está aceptado por la OTI, en concordancia por lo expuesto por la Oficina de Control Interno.

HALLAZGO N° 2. Inobservancia de las Políticas de Seguridad y Privacidad de la información por usuarios del aplicativo Banco de Proyectos.

Descripción: Con el fin de **conocer de manera anónima la percepción de los usuarios finales** frente a los lineamientos de seguridad, confidencialidad y disponibilidad de la información que provee el aplicativo Banco de Proyectos, enmarcados en la Política de Seguridad y Privacidad de la Información definidos en la Resolución 0409 de 2019 y sus anexos o documentos relacionados, se seleccionó una muestra aleatoria de cuarenta (40) usuarios del aplicativo para diligenciar una encuesta diseñada por la Oficina de

Control Interno, de los cuales, diecisiete (17) usuarios atendieron la convocatoria y la diligenciaron, y en su análisis se obtuvieron los siguientes resultados:

- Quince (15) usuarios (88% de los encuestados) ingresa al aplicativo a través de la autenticación en Windows mediante “Usuario y Clave Personalizado”, lo cual está de acuerdo con la directriz de la ADR.

- Doce (12) usuarios (71%) mantiene escrita su contraseña, pero en “lugar seguro”, lo cual no corresponde a una buena práctica de seguridad informática, toda vez que, las claves se pueden ver expuestas.

- Once (11) usuarios (65%) indicaron que las contraseñas cumplen con un nivel de complejidad que se ajusta a las buenas prácticas, al estar conformadas por *mayúsculas, minúsculas, números y caracteres especiales*; sin embargo, el 35% restante (seis usuarios) no percibe la misma robustez en las contraseñas.

- Doce (12) usuarios (71%) indicaron que el sistema no está requiriendo el cambio periódico de contraseña.

- Ocho (8) usuarios (47%) manifestaron haber recibido capacitación de seguridad informática por parte de la OTI durante el presente año, mientras que nueve (9) usuarios (53% restante) indicaron no haberla recibido. Situación que llama la atención considerando las recientes capacitaciones virtuales realizadas por la OTI.

Los resultados anteriores evidenciaron que la ADR debe propender por interiorizar en sus funcionarios y/o colaboradores los temas de cultura y sensibilización de las políticas de seguridad.

De otra parte, se identificó una cultura positiva en cuanto al reporte formal de incidentes y/o requerimientos relacionados con la operación del aplicativo Banco de Proyectos, por cuanto doce (12) usuarios (71% de los encuestados) afirmaron realizar formalmente dicho reporte o requerimiento

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Desconocimiento o falta de interés por parte de funcionarios y contratistas en temas de seguridad de la información. ▪ Insuficiencia de recurso humano en la Oficina de Tecnologías de la Información a raíz de restricciones presupuestales o requerimientos de perfiles específicos que dificultan la asignación y distribución de las labores de Seguridad de la Información. ▪ Desarticulación del Modelo de Seguridad y Privacidad de la información frente a los procesos.	▪ Incumplimiento legal de normas/leyes internas y externas aplicables a los procesos de ADR. ▪ Acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos. ▪ Falla humana en la ejecución de los procesos al desconocer u omitir los lineamientos de seguridad implementados por la ADR, que deriven en pérdida de seguridad y privacidad de la información.	▪ Fuga o robo de información, acceso abierto a datos o a información reservada, confidencial o restringida por parte de terceros no autorizados. ▪ Uso inadecuado de información. ▪ El acceso a información sensible puede facilitar la realización de fraude e impactar en la imagen de la ADR.

Recomendación(es): La implementación de políticas y procedimientos supone un cambio cultural, así como nuevos procesos, por lo tanto, éstos deben ser conocidos y asumidos por quienes hacen uso de los recursos informáticos de la Agencia de Desarrollo Rural (ADR). Es por esto, que se debe realizar de manera permanente campañas de sensibilización en toda la Entidad, tanto a funcionarios, contratistas y a la Alta Dirección.

Con base en los resultados de las encuestas realizadas por la OTI como parte de su plan de capacitación y la llevada a cabo por la Oficina de Control Interno, es necesario establecer un programa que complemente el existente, y que atienda las debilidades identificadas, como son el uso correcto de los dispositivos físicos que brinda la Agencia para el desarrollo de las actividades (cuando se está en sitio), Uso de File Server, procedimientos de TI, uso de claves, entre otros.

Además, es importante realizar una medición del conocimiento adquirido o reforzado a través de las capacitaciones dadas por la OTI, en las cuales participe el 100% de los asistentes, esto le dará a la OTI una visión más amplia de las fortalezas y puntos a mejorar o fortalecer en temas de cultura de seguridad informática; aspecto que también contribuirá a la mejora continua del Modelo de Seguridad y Privacidad de la Información.

Respuesta del Auditado: Aceptado Parcialmente.

Justificación: "*Aunque el desconocimiento o ignorancia de la ley (Resolución 409 de 2019) no sirve de excusa, porque rige la necesaria presunción de que, habiendo sido promulgada, han de conocerla todos. Sobre esta premisa les es imposible a las personas manifestar que no cumplieron con la ley porque no la conocían, máxime cuando por razón al cargo que desempeñan, deben conocerla, sopena de incurrir en negligencia. Es de aclarar que, se ha contado con los recursos profesionales y tecnológicos necesarios, alineados al plan de sensibilización anual propuesto, el cual apoya la Oficina de Comunicaciones y Talento Humano, todo esto en el cumplimiento del MSPI en implementación en la ADR. No obstante, se acepta el hallazgo parcialmente dado que la Oficina de Tecnologías de la Información está comprometida con la política de gobierno digital, en el dominio de uso y apropiación se tiene como entregable Documentar la "Estrategia de Uso y Apropiación de Tecnologías de la Información" para los proyectos de TI que se realizan en la ADR, alineados a PETI y en lo que se refiere a los planes de socialización, para el uso y apropiación se incluirán los de sensibilización de seguridad digital, por lo cual, se realizará un plan de mejora para el cumplimiento en la entrega de la estrategia incluidos los planes de sensibilización de seguridad Digital*."

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Reducida participación de los funcionarios y contratistas en las capacitaciones de la entidad, incluido el personal que interactúa con el sistema de información Banco de Proyectos en lo referente a la seguridad de la información y la aplicación de los lineamientos de la política de seguridad y privacidad de la información.
- Falta de entrega de la información por diferentes oficinas o direcciones de la ADR para consolidar y custodiar la información, aunque se tenga capacidad tecnológica para almacenar.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Elaborar la estrategia de uso y apropiación en la ADR con el fin de vincular a los funcionarios y contratista en el desarrollo de una cultura o comportamientos culturales que faciliten la adopción de tecnología que es esencial para que los proyectos en TI sean productivos; para ello se requiere realizar actividades de fomento en el entorno de formación y sensibilización que logren un mayor nivel de uso y apropiación incluidos los temas de seguridad digital.	Documento Estrategia de Uso y Apropiación de Tecnologías de la Información incluido el plan de sensibilización anual de seguridad digital.	Correctiva	Equipo Humano OTI	20-ene-2021	31-mar-2021

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado con observaciones.

Una vez analizada la información remitida por los responsables de la unidad auditada designados para atender la auditoría, la Oficina de Control Interno precisa que:

El sustento y justificación indicados no desvirtúan las situaciones identificadas por el equipo auditor y presentadas en este hallazgo. Desde la OTI se distingue el compromiso con las gestiones requeridas para la implementación de un marco de seguridad y privacidad de la información aplicables a la ARD, alineado con los requisitos de MinTIC, los cuales dan cumplimiento a la norma ISO 27001:2013. No se identifica la razón por la que se aduce la aceptación parcial, toda vez que, se confirma que a partir de la elaboración de la estrategia de uso y apropiación en la ADR se requiere de un proceso de sensibilización y divulgación a los funcionarios y contratistas.

La Oficina de Control Interno reitera la importancia de la participación de la Alta Dirección en el proceso de apropiación, a través de un liderazgo visible que refuerce la meta establecida por la OTI en el plan de acción, el cual puede realizar mediante comunicaciones regulares que demuestren su compromiso, reiterando a funcionarios y contratistas su responsabilidad frente a lo que conlleva la transformación digital.

Con base en lo anterior, se considera pertinente aclarar que en los archivos de la Oficina de Control Interno reposan los registros (digitales y/o virtuales), papeles de trabajo y demás evidencias que soportan las afirmaciones contenidas en este hallazgo, los cuales se encuentran disponibles para consulta de las partes interesadas, previa solicitud formal de las mismas.

HALLAZGO N° 3. Incumplimiento de los lineamientos procedimentales establecidos para la creación de cuentas en el Directorio Activo.

Descripción: Con base en la información proporcionada por la Oficina de Tecnologías de la Información, respecto a los usuarios creados en el Directorio Activo y que acceden al aplicativo Banco de Proyectos, con corte al 31 de julio de 2020 se pudo identificar que para el periodo auditado se crearon 53 cuentas, de las cuales, la Oficina de Control Interno seleccionó una muestra de quince (15) para validar el cumplimiento de los requisitos establecidos en el procedimiento Administración de usuarios y sistemas de información (PR-GTI-006) versión 1, para la creación de los usuarios de la ADR en el Directorio Activo, para lo cual se solicitaron y validaron los siguientes soportes:

- Existencia de registro del caso en Aranda: solicitud de creación de usuario.
- Formato Solicitud de Servicios TIC (F-GTI-001) debidamente diligenciado
- Evidencia del acta de inicio o acto administrativo de nombramiento: Documento soporte de la solicitud (dependiendo del tipo de vinculación: Planta/Contratista).

Resultado de esta validación, se identificó que de los quince (15) requerimientos de creación de cuenta de usuario, solo tres (3) de ellos (20% de la muestra) cumplieron con los requisitos establecidos; para los doce (12) casos restantes se relacionan a continuación las desviaciones identificadas, las cuales se pueden dar de forma individual o en conjunto varias de ella en un mismo requerimiento de creación:

- En dos (2) casos el Formato Solicitud de Servicios TIC (F-GTI-001) se encontró sin firma.
- En dos (2) el Formato Solicitud de Servicios TIC (F-GTI-001) no contenía fecha del requerimiento.
- En cinco (5) no se evidenció Acta de Inicio o Acto Administrativo de Nombramiento (según corresponda).
- De tres (3) no se entregó Formato Solicitud de Servicios TIC (F-GTI-001).
- De un (1) caso no se entregó evidencia de su registro en Aranda
- De un (1) caso no se suministraron los tres (3) soportes requeridos.
- Se observaron dos (2) soportes (Formato Solicitud de Servicios TIC y Acta de Inicio) con fechas posteriores a la creación del usuario.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Desconocimiento o incumplimiento de las directrices establecidas en el procedimiento Administración de Usuarios y Sistemas de Información (PR-GTI-006), para la creación de usuarios en el Directorio Activo, como acceso principal para los usuarios del aplicativo Banco de Proyectos, al no realizar una revisión cuidadosa de los Formatos Solicitud de Servicios TIC. ▪ Falta de control de monitoreo de los soportes correspondientes a la creación de usuarios según lo establecido en el procedimiento PR-GTI-006.	▪ Fuga de información a causa de accesos no autorizados al sistema. ▪ Acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos.	▪ Fuga o robo de información, acceso abierto a datos o a información reservada, confidencial o restringida por parte de terceros no autorizados. ▪ Uso inadecuado de información.

Recomendación(es): La Oficina de Control Interno recomienda las siguientes alternativas para fortalecer la implementación de actividades de control en el proceso de creación de usuarios en el Directorio Activo (aplica para la gestión de creación, modificación e inactivación de los usuarios de la Agencia de Desarrollo Rural - ADR, para

los servicios de red, correo electrónico y sistemas de información administrados por la Oficina de Tecnologías de la Información):

- Asegurar que para todos los usuarios creados en el Directorio Activo y con acceso al aplicativo Banco de Proyectos, se tengan las autorizaciones y soportes definidos en el procedimiento Administración de Usuarios y Sistemas de Información (PR-GTI-006), para garantizar que todos los usuarios del sistema están autorizados.

- Teniendo en cuenta que para el 86% de los casos revisados se presentaron inconsistencias a nivel de soporte documental, se deberá capacitar al personal de apoyo que realiza las revisiones previas a la creación de cuenta de usuario, para su correcta validación y análisis.

- Se deberán establecer mecanismos eficaces de gestión para el almacenamiento de los soportes (requisitos) establecidos en el procedimiento de Administración de Usuarios, con el fin de disponer de manera organizada y oportuna de esta información, para ello, se pueden considerar las disposiciones aplicables de la "*Guía N° 6 - Gestión Documental*" de MinTIC en el apartado 4 "*Normatividad Técnica Colombiana Sobre Gestión Documental",* la cual incluye información física como electrónica.

- Implementar mecanismos que permitan tener trazabilidad de la creación de cuentas, en especial, para la renovación de cuentas de contratistas, de tal forma que, se pueda establecer con claridad los períodos en los cuales se le ha creado o reactivado la cuenta.

Respuesta del Auditado: Aceptado

Justificación: "*La OTI ha identificado falencias en la creación de cuentas de usuarios dentro del Directorio Activo, por lo tanto, durante la vigencia 2020 se han realizado mejoras sobre el procedimiento, con el fin de establecer puntos de control para asegurar el cumplimiento de éste. Durante el mes de agosto de 2020 se efectuó la actualización del procedimiento DE-GTI-005 que tiene como título "Gestión de Incidentes y*

Requerimientos Tecnológicos"; sin embargo, es importante efectuar ejercicios de socialización y apropiación de los supervisores, funcionarios y contratistas, con el fin de garantizar la correcta ejecución de estas actividades."

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Falla en el diligenciamiento de los formatos que hacen parte de la solicitud de servicios tecnológicos.
- Deficiencia en control de monitoreo de los soportes correspondientes a la creación de usuarios según lo establecido en el procedimiento PR-GTI-006.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Campañas de socialización de los formatos y recomendaciones para la solicitud de servicios tecnológicos.	Realizar una Campaña trimestral (infografía enviada por correo electrónico)	Preventiva	Equipo Humano OTI	20-ene-2021	31-mar-2021
En el procedimiento Administración de Usuarios y Sistemas de Información, específicamente en la actividad N° 4 se tiene proyectado una actualización de eliminación de usuarios; adicional a esto, se incluirá en el "Formato Solicitud de Servicios TIC" (F-GTI-001) la nota aclaratoria donde se solicita su completo diligenciamiento, el cual será devuelto en el caso de no cumplir con este requerimiento. Además, realizar control desde la mesa de servicio siendo esta el único punto de contacto, donde se identifique en el primer nivel la completitud de los campos relacionados en el formato F-GTI-001 y los respectivos soportes que se encuentran descritos en el procedimiento Gestión de Incidentes y Requerimientos Tecnológicos.	Actualización del "Formato Solicitud de Servicios TIC", seguimiento a la completitud de su diligenciamiento y a los soportes respectivos.	Correctiva	Equipo Humano OTI	20-oct-2020	31-dic-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con observaciones.

Analizado el plan de mejoramiento propuesto por los responsables de la unidad auditada, la Oficina de Control Interno lo acepta en razón a que las acciones de mejoramiento establecidas guardan correspondencia con las causas determinadas para este hallazgo; no obstante, recomienda completarlo con capacitaciones al personal de mesa de servicios, de tal manera que, el personal de apoyo tenga claridad en los requisitos definidos para la creación de cuenta, debido a que ésta es el único punto de contacto, donde se valide la completitud de los requisitos establecidos por la ADR en el "Formato Solicitud de Servicios TIC" (F-GTI-001).

HALLAZGO N° 4. Ausencia de lineamientos para la gestión de cuentas de usuario del Directorio Activo a nivel de Eliminación.

Descripción: El 4 de septiembre de 2020, la Oficina de Control Interno fue informada que una vez la cuenta del usuario se deshabilita en el Directorio Activo, la directriz que se tiene es dejarla un mes en la Unidad Organizacional, y pasado este tiempo, si no hay novedad, se lleva a una carpeta de "Cuentas Deshabilitadas" del Directorio Activo. Es importante precisar que, la Entidad no cuenta con un lineamiento formalmente documentado y publicado al respecto.

Con base en la información proporcionada por la Oficina de Tecnologías de la Información (OTI) con corte al 31 de julio de 2020, a través de listados de usuarios a nivel del aplicativo Banco de Proyectos y del Directorio Activo, la Oficina de Control Interno realizó cruces de datos entre ellos para identificar consistencia en la información y en la gestión de los usuarios del aplicativo Banco de Proyectos y del Directorio Activo, validando que no se tuvieran cuentas de usuarios habilitadas para funcionarios y/o contratistas retirados de la Agencia.

Resultado de la evaluación, se identificaron 317 usuarios en el aplicativo Banco de Proyectos que no se encontraban en el listado de Directorio Activo provisto por la OTI. Al

respecto, el 18 de septiembre de 2020, la OTI indicó que: […] "*efectivamente se encuentra que 317 cuentas no están, dado que el día 23 de mayo de 2020 se realizó una eliminación de cuentas que se encontraban en la Unidad Organizacional del Directorio Activo "Cuentas Deshabilitadas" para mejorar el rendimiento en cuanto a la búsqueda de usuarios, para lo cual se propuso un control de cambios*".

De lo anterior, la Oficina de Control Interno obtuvo copia de un "Formato Requerimiento de Cambio" sin código de formato y con fecha 21 de mayo de 2020, mediante el cual se realizó el control de cambios (Consecutivo N° 05-01) de "*Eliminación de cuentas deshabilitadas y no utilizadas*", indicando en el campo "*11. Justificación y beneficios del cambio*", lo siguiente: "*Con la eliminación de estos usuarios se busca mejorar la seguridad y el rendimiento de Active Directory, y también puede ahorrar el tiempo de consulta al no tener que utilizar herramientas y scripts de línea de comandos*".

Aun cuando el formato anterior permitió tener trazabilidad sobre la eliminación masiva de las cuentas reportadas a nivel de Directorio Activo, éste a la fecha de la solicitud no contaba con codificación, lo que indicó que no había sido aprobado ni adoptado a través del Sistema Integrado de Gestión (aplicativo ISOLUCIÓN); además, el formato revisado no contenía las firmas que dieran cuenta de un flujo de elaboración, revisión y aprobación, y no se consideró el registro y soporte del requerimiento en la mesa de servicios (aplicativo ARANDA), así como la notificación al Profesional Especializado Seguridad Informática, quien por sus funciones debe conocer este tipo de cambios. De otra parte, en el *Plan Rollback* no se especificó el motivo de no poder realizar Rollback[4] en caso de error quedando a juicio del lector su interpretación.

[4] En tecnologías de base de datos, un rollback o reversión es una operación que devuelve a la base de datos a algún estado previo. Una reversión es la operación de restaurar una base de datos a un estado anterior mediante la cancelación de una transacción o conjunto de transacciones específico. Soluciones en https://support.microsoft.com/en-us/office/restore-a-previous-version-of-an-item-or-file-in-sharepoint-f66dbda0-81f4-4d1e-b08c-793265c58934

Cabe mencionar que, el 4 de septiembre de 2020 entró en vigencia el procedimiento Gestión de Cambios Tecnológicos (DE-GTI-006) acompañado del *"Formato de Requerimiento de Cambio"*; no obstante, éstos no dan lineamientos específicos para la *Gestión de Cuentas de usuario del Directorio Activo a nivel de Eliminación.*

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Ausencia de lineamientos formales para la gestión de cuentas de usuario del Directorio Activo como la eliminación masiva de usuarios en los sistemas de información. ▪ Falta de depuración oportuna de usuarios bloqueados en el directorio activo, afectando el rendimiento del servicio.	▪ Errores en la ejecución de procesos que impidan la disponibilidad de la información. ▪ Fallas tecnológicas en el aplicativo Banco de Proyectos y/o en la infraestructura técnica (hardware, redes y comunicaciones) que lo soporta, que afecta la seguridad de la información.	▪ Errores en la operación. ▪ Incapacidad de retornar a la operación normal.

Recomendación(es): La Oficina de Tecnologías de la Información debe definir lineamientos formales para la Gestión de Cuentas de usuario del Directorio Activo a nivel de Eliminación, con base en los requisitos propios de la Agencia y en lo aplicable de la Guía N° 3 "Procedimientos de Seguridad de la Información" del MinTIC, los cuales contengan como mínimo:

- Procedimiento a seguir según las tareas requeridas para la gestión de cuentas en el Directorio Activo.
- Flujo de aprobación requerido.
- Procedimientos de Rollback, en caso de error.
- Definición de soportes que deban ser almacenados y/o custodiados.

Con base en el documento a generar sobre gestión de cuentas de usuario del Directorio Activo, realizar validación cruzada con el procedimiento Gestión de Cambios Tecnológicos (DE-GTI-006), con el fin de complementar y referenciar lo aplicable.

Respuesta del Auditado: Aceptado parcialmente

Justificación: "*Se identifica que la OTI tiene el documento PR-GTI-006 con la descripción "Administración de Usuarios y Sistemas de Información", el cual requiere ser actualizado con el instructivo de "Eliminación de cuentas de Directorio Activo" que se encuentra en producción, para mejorar la seguridad y el rendimiento en cuanto a búsquedas de usuarios en esta herramienta administrativa.*

Esta depuración se documentará en el procedimiento de "Administración de Usuarios y Sistemas de Información", adicional a esto, se identifica que este cambio será etiquetado como un cambio estándar, el cual no requiere ser escalado al grupo de cambios de TI.

La ejecución de un Roll-Back para restaurar cuentas eliminadas del Directorio Activo no puede ser ejecutada con la infraestructura actual de la Entidad, puesto que, el sistema operativo instalado no puede actualizarse a una versión que permita habilitar la papelera de reciclaje, adicional a ello existen sistemas de información críticos para la operación (ORFEO, Ulises, IPDR, PDRET) dispuestos en esta infraestructura, que en el caso de ser actualizada la plataforma pueden presentar fallas críticas."

Causa(s) identificada(s) por el Responsable de la Unidad Auditada: Ausencia de lineamientos relacionados con la gestión de usuarios donde se involucre el ciclo de vida de la creación, gestión y eliminación de usuarios dentro del Directorio Activo.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Instructivo con el ciclo de vida de los usuarios del Directorio Activo, en el cual se relacione el flujo de gestión, roll-back, tareas definidas para la administración de usuarios y los respectivos soportes que hacen parte de la gestión del Directorio Activo.	Documentar los lineamientos de eliminación de usuarios	Correctiva	Equipo Humano OTI	5-oct-2020	31-dic-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con observaciones.

Una vez analizada la información remitida por los responsables de la unidad auditada designados para atender la auditoría, la Oficina de Control Interno precisa que, el sustento y justificación indicados no desvirtúan las situaciones identificadas por el equipo auditor y presentadas en este hallazgo, por el contrario, las ratifican. Adicionalmente, no se identifica la razón por la que se aduce la aceptación parcial, toda vez que, se confirma que documentará la depuración de cuentas a nivel de Directorio Activo, así como el etiquetado que se le dará y la documentación requerida (situación que está descrita en el hallazgo), por lo que, se considera pertinente aclarar que en los archivos de la Oficina de Control Interno reposan los registros (digitales y/o virtuales), papeles de trabajo y demás evidencias que soportan las afirmaciones contenidas en este hallazgo, los cuales se encuentran disponibles para consulta de las partes interesadas, previa solicitud formal de las mismas.

HALLAZGO N° 5. Inadecuada gestión y monitoreo de usuarios y roles asignados en el aplicativo Banco de Proyectos.

Descripción: De acuerdo con lo establecido en la Guía N° 8 “Controles de Seguridad y Privacidad de la Información” del MinTIC, la cual se encuentra alineada con la Norma ISO 27001:2013, numeral A.9.2.2 “*Suministro de acceso de usuarios*”, cuyo control sugiere que “*se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar* [revocar] *los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios*”, la Oficina de Control Interno con base en la información proporcionada por la Oficina de Tecnologías de la Información (OTI) con corte al 31 de julio de 2020, a través de listados de usuarios a nivel del aplicativo Banco de Proyectos y del Directorio Activo, realizó cruces de datos entre ellos para identificar consistencia en la información y en la gestión de los usuarios, así:

a. Aplicativo Banco de Proyectos y del Directorio Activo, validando que no se tuvieran accesos habilitados en el aplicativo para funcionarios y/o contratistas retirados de la Agencia. Al respecto, se identificaron 317 cuentas sin gestión en el aplicativo Banco de Proyectos que correspondían a usuarios retirados de la ADR (funcionarios y/o contratistas), y que si bien se inactivaron desde el Directorio Activo, aún continuaban con rol vigente en el aplicativo. Se identificó que esta situación se originó al no reportar a la(los) funcionaria(os) encargados de administrar los accesos y novedades en el aplicativo sobre los retiros de funcionarios y/o contratistas. Con base en lo anterior, se concluye que no se ha efectuado un proceso de revisión y depuración de usuarios y roles asignados, y que no se cuenta con lineamientos para su realización que garanticen una correcta gestión de usuarios y segregación funcional, basándose en los principios de "menor privilegio, necesidad-de-tener y necesidad-de-conocer r"[5].

   Adicionalmente, se confirmó con los responsables del aplicativo Banco de Proyectos, que no se ha realizado revisión de la matriz de roles entregada por el proveedor, lo cual es sugerido por la norma ISO 27001:2013, en el anexo A.9.2.5 "*Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares*".

b. Se identificaron once (11) cuentas genéricas activas para Banco de Proyectos que inician con las palabras "migra" y "migración", de las cuales, se tuvo conocimiento que siete (7) de ellas fueron solicitadas vía correo electrónico del 29 de agosto de 2018 por el funcional del aplicativo, para ser usadas por él mismo como encargado de efectuar la migración al aplicativo de las iniciativas de proyectos que se encontraban en documentos físicos; y de las cuatro (4) cuentas restantes que fueron creadas en mayo de 2019 no se obtuvo soporte de solicitud y no tenían funcionario responsable. De acuerdo con los requisitos establecidos en el procedimiento "Administración de usuarios y sistemas de información" (PR-GTI-006) versión 1, los responsables de las

[5] Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión. Dominio DSS05.04: Gestionar la identidad del usuario y el acceso lógico.

dependencias son los autorizados para efectuar dicha solicitud. Al cierre de la prueba de auditoría no se obtuvo evidencia del requerimiento que se debió efectuar parte de la Vicepresidencia de Proyectos a la OTI.

c. El Anexo A.9.2.3 "*Gestión de derechos de acceso privilegiado*" de la Norma ISO 27001:2013 establece como control: "*Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado*"; no obstante, en la revisión efectuada se identificaron ocho (8) cuentas (activas) con rol "Administradores" para la aplicación Banco de Proyectos, de las cuales, siete (7) de ellas pertenecían a la OTI y una (1) al funcional de la Vicepresidencia de Proyectos, de estas cuentas, si bien se conocía el responsable, no todas estaban soportadas y documentadas formalmente en cuanto a su uso.

   Adicionalmente, no se identificó la aplicación del lineamiento para la administración y custodia de la clave asignada al súper usuario "banco.proyectos" (constancia, registro, transferencia), considerando que esta cuenta tenía todos los permisos de administración en la aplicación, y fue configurada directamente por el proveedor.

d. Se identificaron roles operativos asignados a personal de la OTI pertenecientes a la Unidad Organizacional "*ADR_Users / Presidencia / Oficina de Tecnologías de la Información*" (cuatro casos), lo que genera conflicto entre quien administra y ejecuta la actividad.

Adicionalmente, con el fin de validar las actividades realizadas en el sistema por parte de las cuentas genéricas, cuentas a cargo de personal de la OTI con privilegios de Administrador y cuentas OTI con roles operativos, se requirió a los funcionarios asignados al "*Equipo Banco de Proyectos"* realizar consulta sobre estas cuentas, a lo que indicaron que, si bien el sistema permitía generar los logs, en el momento no se conocía la estructura de éstos, situación que representó una limitación en la validación de las actividades realizadas (trazabilidad). Esta situación se detalla en el Hallazgo N° 8.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Estado de madurez del Modelo de Seguridad y Privacidad de la ADR en proceso de fortalecimiento. ▪ Ausencia de lineamientos formales para la gestión de cuentas de usuario a nivel de aplicación. ▪ Falta de control de monitoreo de los soportes correspondientes a la creación de usuarios según lo establecido en el procedimiento PR-GTI-006. ▪ Ausencia de lineamientos para el monitoreo de privilegios otorgados a los usuarios en el aplicativo.	▪ Incumplimiento legal de normas/leyes internas y externas aplicables a los procesos de ADR. ▪ Acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos. ▪ Falla en la operatividad en el aplicativo Banco de Proyecto, para el módulo de Proyectos, Evaluación y Calificación. ▪ Calificación y evaluación de proyectos por parte de los servidores de la ADR no ajustados a los criterios definidos para favorecimiento con recursos públicos a un tercero o para beneficio propio. ▪ Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero.	▪ El acceso a información sensible puede facilitar la realización de fraude e impactar en la imagen de la ADR. ▪ Fuga o robo de información, acceso abierto a datos o a información reservada, confidencial o restringida por parte de terceros no autorizados. ▪ Uso inadecuado de información.

Recomendación(es): Definir un procedimiento para la revisión periódica de los usuarios y los roles otorgados en el aplicativo, así como de la matriz de roles que es base para otorgar los accesos en el aplicativo. El lineamiento debe establecer, entre otros, los siguientes aspectos:

- Alcance.
- Periodicidad de ejecución.
- Responsabilidades en el proceso para el Grupo Banco de Proyectos y para las áreas que solicitan acceso al aplicativo.
- Inactivación de permisos en el aplicativo para funcionarios retirados,
- Segregar, reducir al mínimo necesario y gestionar activamente cuentas de usuario privilegiadas, como son las cuentas de super usurarios y usuarios administradores. Asegurar la supervisión de todas las actividades en estas cuentas.

- Asegurar el cumplimiento del lineamiento de custodia (constancia, registro, transferencia) de contraseña de la cuenta “super usuario”

- Documentar cuentas requeridas para la ejecución de procesos propios del sistema

- Documentación a almacenar como evidencia de ejecución del procedimiento

Como medida mitigante, inicialmente se puede incluir en el proceso de reporte de retiro de personal perteneciente a las Unidades Organizacionales que acceden el Banco de Proyectos “*ADR_Users / Vicepresidencia de Integración Productiva, ADR_Users / Vicepresidencia de Proyectos, y ADR_Users / Vicepresidencia de Gestión Contractua*l”, copia a las direcciones de correo electrónico de los administradores del aplicativo Banco de Proyectos, para que éstos realicen oportunamente las actividades de gestión de usuarios en el sistema.

Para las cuentas genéricas, cuentas con rol “Administradores” y cuentas de funcionarios OTI con privilegios a la operatividad del sistema, revisar los casos reportados, realizar el análisis de la causa raíz de las situaciones observadas y, de ser necesario, establecer controles adicionales que impidan excepciones en el cumplimiento del procedimiento de asignación de roles; para ello, se puede establecer una revisión cruzada entre los administradores para detectar desviaciones en el cumplimiento del proceso y corregirlas oportunamente.

Respuesta del Auditado: Aceptado Parcialmente.

Justificación: “*Si bien se aceptan los hallazgos que se evidenciaron, dejamos claro que no estamos de acuerdo con la descripción de Riesgos y con la descripción de los Impactos, teniendo en cuenta que no hay relación de usuarios y roles con los riesgos y los impactos evidenciados.*

- *Acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos.*

- *Falla en la operatividad en el aplicativo Banco de Proyecto, para el módulo de Proyectos, Evaluación y Calificación.*
- *Calificación y evaluación de proyectos por parte de los servidores de la ADR no ajustados a los criterios definidos para favorecimiento con recursos públicos a un tercero o para beneficio propio.*
- *Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero.*
- *El acceso a información sensible puede facilitar la realización de fraude e impactar en la imagen de la ADR.*
- *Fuga o robo de información, acceso abierto a datos o a información reservada, confidencial o restringida por parte de terceros no autorizados.*

En el sistema de Banco de Proyectos se desarrollan actividades en donde se inicia la creación de una iniciativa, se estructuración y la viabilizan para la ejecución, es este sistema no se maneja recursos de la ADR, solo se guarda información."

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Estado de madurez del Modelo de Seguridad y Privacidad de la ADR en proceso de fortalecimiento.
- Ausencia de lineamientos formales para la gestión de cuentas de usuario a nivel de aplicación.
- Falta de control de monitoreo de los soportes correspondientes a la creación de usuarios según lo establecido en el procedimiento PR-GTI-006.
- Ausencia de lineamientos para el monitoreo de privilegios otorgados a los usuarios en el aplicativo.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Garantizar que la información de usuarios que se encuentra en la aplicación Banco de Proyectos este actualizada.	Depurar la base de datos de usuario que está en la aplicación de Banco de Proyectos con los usuarios que se encuentran en el Directorio Activo.	Correctiva	Equipo Humano OTI	01-nov-2020	30-dic-2020
Definir la matriz de Roles de la aplicación Banco de Proyectos	Revisar e identificar la matriz de Roles entregada por el proveedor y capacitar a los usuarios.	Correctiva	Equipo Humano OTI	01-nov-2020	30-dic-2020
Modificación del formato de solicitud de servicios TIC de la OTI.	Incluir en el formato de solicitud de servicios TIC el campo de permiso del Rol cuando soliciten activar usuario en el Banco de Proyectos.	Correctiva	Equipo Humano OTI	01-nov-2020	30-dic-2020
Diseñar el procedimiento de permisos de roles usuarios en la aplicación del Banco de Proyectos.	Diseñar procedimiento de permisos de Rol de usuarios del Banco de Proyectos.	Correctiva	Equipo Humano OTI	01-nov-2020	01-abr-2021

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con observaciones.

Analizado el plan de mejoramiento propuesto por los responsables de la unidad auditada, la Oficina de Control Interno lo acepta en razón a que las acciones de mejoramiento establecidas guardan correspondencia con las causas determinadas para este hallazgo; no obstante, no se identifica la razón por la que se aduce la aceptación parcial. Al respecto, se precisa que los riesgos e impactos identificados por la Oficina de Control Interno corresponden a lo evidenciado en la auditoría, puesto que no se pudo obtener trazabilidad del cumplimiento de los procedimientos establecidos para la creación de

roles en el aplicativo, materializando el riesgo “incumplimiento legal de normas/leyes internas y externas aplicables a los procesos de ADR”.

Es claro para la Oficina de Control Interno que el aplicativo no maneja recursos financieros; sin embargo, el aplicativo ha sido implementado para contar con un Banco de Proyectos (desde la concepción de las iniciativas), en el que se desarrolla todo el flujo de evaluación y calificación de éstos. Al no efectuar revisión de la matriz de roles y validar periódicamente los accesos otorgados por parte del(los) dueño(s) del(los) proceso(s), es inviable tener certeza que los usuarios no cuenten hoy en día con mayores atribuciones en el sistema, lo que en caso de materializarse podría ocasionar acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos, así como la posible calificación y evaluación de proyectos por parte de los servidores de la ADR no ajustados a los criterios definidos para favorecimiento con recursos públicos a un tercero o para beneficio propio u ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero.

Sumado a lo anterior, se tiene un número importante de cuentas administrativas (siete) que no han sido depuradas o sustentadas en cuanto a su necesidad; no todas están documentadas formalmente en cuanto al uso que se les da; en caso de error humano o al efectuar alguna modificación al aplicativo o un cambio no autorizado, podrían causar fallas en la operatividad en el aplicativo Banco de Proyectos, para el módulo de Proyectos, Evaluación y Calificación.

La Oficina de Control Interno, reitera la importancia de la depuración de las cuentas “Administradores” y las cuentas genéricas “migra y Migración” como prioridad, así como la documentación formal del objetivo de estas cuentas; la acción debe ser incluida puntualmente como parte del plan de mejora.

HALLAZGO N° 6. Deficiencia de controles en el proceso de gestión de cambios sobre el sistema y modificaciones directas a datos en producción.

Descripción: El soporte, mantenimiento y administración de cambios sobre el aplicativo Banco de Proyectos se ejecutó bajo el Contrato N° 456 de 2019 que fue suscrito con PricewaterhouseCoopers (PwC) Asesores Gerenciales Ltda., el cual tenía como objeto "*Contratar la prestación de servicios profesionales para realizar las actividades preventivas, correctivas, de soporte y complementarias a la solución Banco de Proyectos de la Agencia de Desarrollo Rural*", con plazo de ejecución desde el 14 de agosto de 2019 hasta el 31 de diciembre de 2019, y en revisión de los documentos relacionados aportados por la OTI se identificaron las siguientes situaciones:

a. En el Informe de Supervisión fechado 27 de diciembre de 2019, se identificó la solicitud de una prórroga del contrato para el periodo comprendido entre el 01 y 31 de enero de 2020 sustentada en el cambio del procedimiento de estructuración de los PIDAR modificado en su quinta versión aprobado el 6 septiembre de 2019, debido a que el contratista debía realizar ajustes en los módulos a desarrollar. Así las cosas, y con el fin de verificar el estado del contrato (cierre u otro), al corte de 31 de julio de 2020 se solicitaron los siguientes documentos que hacían parte del Contrato N° 456 de 2019, de los cuales, la Oficina de Tecnologías de la Información no aportó las evidencias correspondientes:

   - Otrosí o documento de aprobación y/o formalización de la prórroga solicitada.
   - Sesión de supervisión del contrato, teniendo en cuenta que en la solicitud de la prórroga se requirió cambio de supervisor.
   - Acta de finalización o liquidación del contrato.

b. De acuerdo con lo establecido en la norma ISO 27001:2013, numeral A.14.2 "*Seguridad en los procesos de desarrollo y de soporte*", se debería contar con un procedimiento para el control de cambios sobre los sistemas de información. Al respecto, la Oficina de Control Interno evidenció que la ADR no contaba al 31 de julio de 2020 con una metodología para la Gestión de Cambios Tecnológicos, por lo que

el proceso se realizó con la metodología del proveedor, quien implementó un formato de requerimiento de cambio, el cual debía estar firmado por el líder funcional de ADR y el líder técnico de la ADR. Este formato de control de cambios incluyó, entre otros, los siguientes aspectos:

- Clasificación del cambio
- Afectación
- Efecto del cambio
- Justificación
- Riesgo
- Impacto en otros sistemas
- Plan de implementación
- Plan de Roll Back
- Matriz de Efecto del Cambio

Durante la vigencia del contrato con PwC, y según lo indicado por el Supervisor del contrato, se ejecutaron los siguientes diez (10) cambios sobre la herramienta siguiendo el procedimiento, estructura y formatos establecidos por el proveedor:

ID	FECHA	DESCRIPCIÓN	OBSERVACIÓN OCI
RFC[6]1	21-ago-2019	Implementación y configuración del ambiente de pruebas del Banco de Proyectos de la ADR	Sin observaciones

[6] RFC por sus siglas en ingles Request for Change. El cual corresponde a una Solicitud de Cambio.

ID	FECHA	DESCRIPCIÓN	OBSERVACIÓN OCI
RFC2	04-sep-2019	Ajuste del módulo de personas según solicitud por ADR. Mejorar la experiencia de usuario para la consulta y el registro de personas, disminuyendo los tiempos de respuesta del sistema y mejorando la interacción usuario - sistema.	Sin observaciones
RFC3	04-sep-2019	Ajuste del módulo de personas según solicitud por ADR. Mejorar la experiencia de usuario para la consulta y el registro de personas, disminuyendo los tiempos de respuesta del sistema y mejorando la interacción usuario - sistema.	Sin observaciones
RFC4	06-sep-2019	Debido a la actualización del módulo de personas en el Banco de Proyectos, se requiere ajustar el módulo de asignación de beneficiarios a predios para que se conecte a la nueva estructura de datos, brindando agilidad a la labor de consulta y creación de asignaciones.	No se cuenta con formato firmado
RFC5	20-sep-2019	Desarrollo del Nuevo Landing Page para el Banco de Proyectos - ADR	Sin observaciones
RFC6	23-sep-2019	El formulario de marco lógico contará con un acceso a los predios que se deseen consultar, mejorando de esta manera la experiencia de usuario al consultar en un solo lugar los predios.	No se cuenta con formato firmado
RFC7	25-nov-2019	Realizar ajuste a nivel de aprobaciones en el formulario de marco lógico, según solicitud realizada por el líder funcional.	No se cuenta con formato firmado Inconsistencia en la fecha vs consecutivo
RFC8	25-sep-2019	Ampliar la capacidad de almacenamiento de la granja de SharePoint en la cual se encuentra alojada la solución Banco de Proyectos, así como redistribuir el contenido de la base de datos de contenido de SharePoint, lo anterior con el fin ampliar la vida útil del mismo y mejorar el tiempo de respuesta en consulta y escritura de la información.	Sin observaciones
RFC9	20-sep-2019	Desarrollar y aplicar los nuevos ajustes de diseño, en las etapas de ejecución y supervisión.	Sin observaciones
RFC10	23-sep-2019	Desarrollar los formularios del proceso de Estructuración del Banco de Proyectos en .Net adicionando los campos de asistencia técnica y conservando los campos que se encuentran actualmente en dichos formularios.	Sin observaciones

***Fuente**: Construcción Propia de la Oficina de control Interno, con base en los RFC proporcionados por la OTI.*

La OTI dispuso los soportes relacionados, tanto con los RFC como los de la ejecución de pruebas que se realizaron el 16 de diciembre de 2019 sobre el módulo de personas del aplicativo Banco de Proyectos; sin embargo, al cruzar la información no se evidenciaron los soportes de los RFC relacionados para el paso a producción de este módulo.

Adicionalmente, se identificó que durante el periodo auditado se implementaron tres (3) cambios en torno al aplicativo Banco de Proyectos, relacionados con la migración del servidor y las tres (3) máquinas virtualizadas a la nube:

ID	FECHA	DESCRIPCIÓN
1	16-jul-2020	Se modificará el archivo WEB.CONFIG que se encuentra en la ruta "C:\Users\banco.proyectos\source\repos\BancoProyectosADRV2\BancoProyectosADR" del servidor "SRVBANPROYAPP01", para que la cadena de conexión a la base de datos no se realice por dirección IP sino lo haga por nombre de registro DNS.
1	23-jul-2020	Se realizará migración de los servidores srvbanproyapp01, srvbanprowfe01 y srvbanproysql01 de la infraestructura que se tiene en el Datacenter que se encuentra en la ADR a la plataforma en la nube de Microsoft Azure.
1	24-jul-2020	Se realizará migración de los servidores srvbanproyapp01, srvbanprowfe01 y srvbanproysql01 de la infraestructura que se tiene en el Datacenter que se encuentra en la ADR a la plataforma en la nube de Microsoft Azure.

Nótese que los tres controles de cambio revisados presentan el mismo número de identificación (ID), y los dos últimos RFCs fechados con 23 y 24 de julio de 2020 registran la misma descripción de cambio.

Dentro de los documentos suministrados no se evidenciaron soportes de ejecución de pruebas y resultados de las mismas; a la vez que no fue posible realizar correlación entre los casos de ARANDA y los RFC entregados.

c. En revisión del documento “Manual Administración del Banco de Proyectos” versión 1 del 5 de diciembre de 2019, entregado a la ADR por parte del proveedor, la Oficina de Control Interno evidenció al menos tres (3) casos en los que PwC indica que deben ser manejados por OTI y registrados en ARANDA, a saber:

- Cambio de estado en formulario.
- Recuperación de archivos adjuntos.
- Atención de casos con el uso de Share Point Designer

Sin embargo, la documentación de los casos es muy básica en la herramienta ARANDA, debido a que, entre otros aspectos, no se logra dar una correcta tipificación de los casos y una clara descripción de la solución.

Aunado a lo anterior, en reunión del 3 de septiembre de 2020 con los Ingenieros de la OTI y el Equipo Banco de Proyectos, se conoció que se han realizado ajustes manuales a los Formularios "XML" que se manejan en el aplicativo cuando se presentan daños en éstos, y que para tal fin, el proveedor los ha capacitado porque éstos ajustes solo deben ser realizados por los ingenieros OTI. Así mismo, en sesión con los delegados de la Vicepresidencia de Proyectos para la auditoría, la Oficina de Control interno conoció que se han realizado cargas manuales de listas de beneficiarios a iniciativas cuando éstas contienen un gran número de participantes.

Considerando la documentación entregada por la OTI, para la Oficina de Control Interno no es posible garantizar que durante el periodo evaluado no se hayan implementado otros cambios diferentes a los proporcionados por la OTI; esto sumado a que se desconoce por parte del equipo de Banco de Proyectos una funcionalidad del sistema que permita extraer un reporte donde se identifiquen los cambios o modificaciones directas a datos en ambiente productivo para un periodo de tiempo determinado, donde se evidencie fecha, usuario, modificación y estado del mismo.

En cuanto al manejo de versiones del aplicativo Banco de Proyectos, se informó que no se cuenta con una base histórica de versiones (hoy, Versión 2), de la cual la ADR es propietaria de los códigos fuente. Su almacenamiento está en los servidores de los cuales se generan copias de respaldo de acuerdo con el esquema establecido; no obstante, se carece de una base histórica de los cambios que se han efectuado sobre

el código fuente del sistema de información Banco de Proyectos, que permita tener trazabilidad sobre éstos.

d. En la Ley 1581 de 2012 “Protección de Datos Personales” en su Artículo 4 literal h “Principio de confidencialidad”, se establece que *“[…] Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma*.” Con relación a lo anterior, en la Agencia no se identificó un procedimiento para la transformación de datos de producción que son usados para la ejecución de pruebas, en el que se garantice la reserva y restricción de la información; requisito que no se evidenció para las pruebas de la versión 2 del Banco de Proyectos.

e. Con base en los resultados de esta auditoría, se identificaron las siguientes tres (3) situaciones en las cuales se puede requerir apoyo del proveedor, aunque se conoció que una vez finalizado el contrato con PwC no se subscribió contrato de soporte y mantenimiento:

   - Entender la estructura y definición de los logs que tiene predefinidos el aplicativo.
   - Apoyo en la atención de fallas técnicas que se generaron durante la creación de ambiente de pruebas para esta auditoría. Esta situación no permitió recrear el ambiente, afectando el alcance y las pruebas planeadas.
   - Desarrollo e implementación del Acuerdo 10 de 2019, el cual aún está en proceso de revisión y aprobación del Procedimiento.

f. Para la segregación de ambientes de prueba y producción para el cambio de versión 2, de acuerdo con el control de cambios reportado en el RFC1 del 21 de agosto de 2019, se realizó la implementación y configuración del ambiente de pruebas del Banco

de Proyectos de la ADR por parte de PwC, con la siguiente justificación: "*Contar con un ambiente de desarrollo en el cual se puedan realizar despliegues de nuevos componentes, pruebas de funcionamiento, eliminación de componente con el fin de probar resultados. Lo anterior con el fin de no afectar el ambiente productivo*". Una vez finalizada la implementación en productivo, el ambiente de pruebas se suspendió; sin embargo, no se obtuvo evidencia de la fecha suspensión del ambiente, así como de los procedimientos de borrado seguro de los datos usados en el entorno de pruebas y que venían del entorno de producción.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Imposibilidad de generar directamente del sistema Banco de Proyectos un reporte que permita identificar los cambios al sistema o modificaciones directas de datos. ▪ Falta de definición de lineamiento para el registro de los cambios que son aplicados a producción. ▪ Ausencia de lineamientos de los soportes del proceso de gestión de cambios, y almacenamiento centralizado. ▪ Falta de lineamientos para la administración de modificaciones directas a datos en el sistema. ▪ Desconocimiento de las normas de aseguramiento de datos de producción usados en pruebas.	▪ Incumplimiento legal de normas/leyes internas y externas aplicables a los procesos de ADR. ▪ Fallas tecnológicas en el aplicativo Banco de Proyectos y/o en la infraestructura técnica (hardware, redes y comunicaciones) que lo soporta, que afecta la seguridad de la información. ▪ Errores en la ejecución de procesos que impidan la disponibilidad de la información. ▪ Falla en la operatividad en el aplicativo Banco de Proyecto, para el módulo de Proyectos, Evaluación y Calificación. ▪ Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero.	▪ Errores, fallas o incidentes en el sistema que afecten la recuperación y seguridad de la información por cambios en producción que no sean probados, autorizados y certificados. ▪ El acceso y modificación a la información sensible puede facilitar la realización de fraude e impactar en la imagen de la ADR. ▪ Fuga de información confidencial al no realizar transformación o destrucción de información confidencial en los servidores de pruebas al iniciar o finalizar las pruebas. ▪ Indisponibilidad de la información o del servicio para el proceso misional por modificaciones directas a datos de producción no probados y certificados.

Recomendación(es): De acuerdo con las buenas prácticas, se debe definir y ejecutar un proceso de gestión de cambios que garantice el registro en su totalidad y de forma centralizada de las modificaciones que son aplicadas al sistema Banco de Proyectos.

Para ello, se deberá determinar e implementar un procedimiento[7] que garantice la total trazabilidad de los cambios que se lleven a producción para el aplicativo, donde se establezcan y/o formalicen los siguientes aspectos:

- Repositorio centralizado de registro de todos los cambios.
- Procedimiento de gestión de cambios.
- Procedimiento de transformación de datos de producción usados en pruebas.
- Procedimiento para la administración, aprobación y registro de las modificaciones de datos que se realizan directamente en producción.

En el momento en que se requiera, se deberá definir y establecer un entorno de pruebas seguro y representativo, el cual deberá estar disponible en términos de rendimiento, capacidad, seguridad, controles internos, prácticas operativas, calidad de los datos, requisitos de privacidad y cargas de trabajo. Para ello se pueden considerar las siguientes actividades:

1. Crear una base de datos de pruebas que sea representativa del entorno de producción. Borrar en forma segura los datos usados en el entorno de pruebas y que vienen del entorno de producción, conforme a las necesidades del proceso, y a los estándares de la ADR.
2. Proteger los datos de prueba y resultados sensibles contra su divulgación, incluido el acceso, retención, almacenamiento y destrucción.
3. Establecer un proceso que permita la apropiada retención o eliminación (disposición) de los resultados de las pruebas, medios u otra documentación asociada, que permitan la revisión adecuada y el subsiguiente análisis o realización eficiente de

[7] Se sugiere considerar el marco de referencia COBIT 2019, Dominio: Construir, adquirir e implementar. Objetivo de gestión: BAI03 - Gestionar la identificación y construcción de soluciones. Su propósito se enmarca en "Garantizar una prestación ágil y escalable de productos y servicios digitales. Establecer soluciones oportunas y rentables (tecnología, procesos de negocio y flujos de trabajo) capaces de apoyar los objetivos estratégicos y operativos de la empresa."

nuevas pruebas, según lo requiera el plan de pruebas. Considerando los efectos de requisitos de cumplimiento o regulatorios como lo es la ley 1581 de 2012.

4. Garantizar que el entorno de pruebas sea seguro e incapaz de interactuar con el sistema de producción

Algunas métricas que se pueden implementar son:

a. Nivel de comparación entre el entorno de pruebas y el entorno operativo y de negocio futuro.

b. Nivel de datos (y/o bases de datos) de pruebas borrados de forma segura que son representativos del entorno de producción

Es importante formalizar la base histórica de los cambios efectuados al código fuente del sistema de información Banco de Proyectos, toda vez que, esto permite llevar la trazabilidad de los cambios efectuados, corregir futuras fallas y prevenir cambios no autorizados que conlleven a una interrupción y/o disponibilidad del servicio que puedan tener impacto en la operación del sistema y por ende en el registro.

Finamente, es necesario dar celeridad al proceso y finalizar formalmente la relación contractual con PwC mediante el cierre y firma del acta de finalización o liquidación del contrato. Así mismo, recolectar y disponer en la carpeta del proyecto (aplicativo Banco de Proyectos) los documentos que hacen parte del Contrato N° 456 de 2019, como son la sesión de supervisión del contrato y el Otrosí o documento de aprobación de la prórroga.

Respuesta del Auditado: Aceptado.

Justificación: "*Se encuentra que todas las causas expuestas son coherentes con la evidencia y los documentos proporcionados, las cuales en su mayoría corresponden a la falta de implementación del procedimiento de desarrollo de software de la Agencia de Desarrollo Rural, procedimiento implementado luego de la ejecución del contrato.*"

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Imposibilidad de generar directamente del sistema Banco de Proyectos un reporte que permita identificar los cambios al sistema o modificaciones directas de datos
- Falta de definición de lineamiento para el registro de los cambios que son aplicados a producción.
- Ausencia de lineamientos de los soportes del proceso de gestión de cambios, y almacenamiento centralizado.
- Falta de lineamientos para la administración de modificaciones directas a datos en el sistema.
- Desconocimiento de las normas de aseguramiento de datos de producción usados en pruebas

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Contratación para la creación de un reporte según indicaciones por parte de control interno	1 contrato	Correctiva	Equipo Humano OTI	01-feb-2021	31-dic-2021
Aplicación del procedimiento de desarrollo de software, y procedimiento de cambios de tecnología.	1 publicación del procedimiento de desarrollo de software y modificación del procedimiento de cambios de tecnología	Correctiva	Equipo Humano OTI	15-oct-2020	31-dic-2020
Agregar la opción de Datafix en Aranda para la solicitud de éstos.	1 modificación en la clasificación de las solicitudes de Aranda	Correctiva	Equipo Humano OTI	15-oct-2020	31-dic-2020

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Agregar al procedimiento de desarrollo de software un apartado para la anonimización de datos en los ambientes de pruebas.	1 publicación del procedimiento de desarrollo de software	Correctiva	Equipo Humano OTI	15-oct-2020	31-dic-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Al analizar el plan de mejoramiento propuesto por los responsables de la unidad auditada, se identificaron los siguientes aspectos adicionales, que es importante sean considerados para su ajuste y complemento:

- Dar celeridad al cierre contractual con PwC mediante la terminación y firma del acta de finalización o liquidación del contrato. Así mismo, recolectar y disponer en la carpeta del proyecto (aplicativo Banco de Proyectos) los documentos que hacen parte del Contrato N° 456 de 2019, como son la sesión de supervisión del contrato y el Otrosí o documento de aprobación de la prórroga.

- Como parte de la acción "*Agregar al procedimiento de desarrollo de software un apartado para la anonimización de datos en los ambientes de pruebas*", se deberán considerar acciones que le permitan a la ADR garantizar la disponibilidad de un entorno de pruebas en el momento que sea requerido, surtiendo los pasos descritos en el nuevo instructivo de Separación de Ambientes Infraestructura Tecnológica (IN-GTI-002) Versión 1 del 31de agosto de 2020, garantizando que éste sea seguro e incapaz de interactuar con el sistema de producción.

Finalmente, incluir como parte de los planes de acción, la formalización de la base histórica de los cambios efectuados al código fuente del sistema de información Banco de Proyectos, llevando así la trazabilidad de los cambios efectuados.

HALLAZGO N° 7. Deficiencias en documentación y trazabilidad de los casos registrados en la herramienta de mesa de servicios ARANDA.

Descripción: En cuando a la Gestión de Incidentes de Seguridad de la Información, los anexos A.16.1.6 "*Aprendizaje obtenido de los incidentes de seguridad de la información*" y A.16.17 "*Recopilación de evidencia*" de la Norma ISO 27001:2013, indican que:

- A.16.1.6. "*El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.*"

- A.16.1.7. "*La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.*"

No obstante lo anterior, a la fecha de corte del período auditado (31 de julio de 2020) la ADR no contaba con un procedimiento formalizado y divulgado para la "Gestión de incidentes y requerimientos tecnológicos"; aunque se observó que el 6 de agosto de 2020 fue aprobado y publicado en el aplicativo ISOLUCIÓN un procedimiento con código DE-GTI-005 para atender y solucionar incidentes y requerimientos presentados por los usuarios.

Teniendo en cuenta lo anterior, se solicitó a la OTI documentación referente a requerimientos, fallas e incidencias reportadas en la mesa de servicio ARANDA relacionadas con el aplicativo Banco de Proyectos, de lo que suministraron un listado de éstas presentadas durante el período objeto de auditoría (agosto 2019 a julio 2020), y teniendo en cuenta que, esta actividad de control (requerimientos ARANDA) tiene una frecuencia diaria, la Oficina de Control Interno seleccionó una muestra de cuarenta (40) casos, de los cuales se solicitaron los soportes que permitieran evidenciar la trazabilidad del requerimiento desde su solicitud hasta su solución o cierre del caso.

De la muestra seleccionada, la OTI suministró soportes o documentación de doce (12) casos (30% de la muestra), con la que se determinó:

- No fue posible realizar una correlación entre los incidentes reportados en la mesa de servicio y los soportes entregados. La Ingeniera a cargo tuvo que realizar la actividad manualmente.

- No se tiene un repositorio centralizado y organizado de los soportes relacionados a los incidentes de la mesa de servicio que permita realizar una trazabilidad eficiente de todos los casos reportados.

- Dentro de la herramienta no se está dejando el detalle organizado y suficientemente documentado del incidente reportado, que permita identificar el riesgo, la causa del problema, el análisis de la solución y la solución aplicada, debido a que los casos se cierran con “caso cerrado” o “el requerimiento fue solucionado”, sin dejar registro del resultado y afectación de la solución, así como los soportes correspondientes o lugar de almacenamiento de éstos.

- Los mecanismos de gestión de incidencias utilizados no proporcionaron evidencia suficiente de la forma en que los casos fueron atendidos y solucionados, y por consiguiente, de la trazabilidad de las soluciones brindadas.

Si bien el equipo Banco de Proyectos efectúa seguimiento diario de los casos reportados, no se identificó a nivel de mesa de ayuda ARANDA una métrica más allá del promedio de tiempo requerido para la atención, que le permita a la OTI determinar el número y gravedad del incidente reportado para realizar un análisis de los casos más críticos con los soportes de solución y así poder determinar si este es repetitivo o aislado, y poder tomar las medidas pertinentes.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Imposibilidad de realizar trazabilidad a los incidentes reportados en la mesa de servicio. ▪ Falta de definición de lineamiento para el correcto registro (tipificación, definición de impacto, urgencia, prioridad, nombre del SLA, entre otros) de los incidentes en la mesa de servicio. ▪ Desconocimiento de las bondades que ofrece la herramienta. ▪ Ausencia de un repositorio centralizado para el almacenamiento de evidencias de los incidentes reportados.	▪ Fallas tecnológicas en el aplicativo Banco de Proyectos y/o en la infraestructura técnica (hardware, redes y comunicaciones) que lo soporta, que afecta la seguridad de la información. ▪ Errores en la ejecución de procesos que impidan la disponibilidad de la información. ▪ Falla en la operatividad en el aplicativo Banco de Proyecto, para el módulo de Proyectos, Evaluación y Calificación.	▪ Errores o incidentes que afecten la recuperación y seguridad de la información. ▪ Indisponibilidad del servicio para un proceso misional debido a errores repetitivos no solucionados de raíz. ▪ El acceso a información sensible puede facilitar la realización de fraude e impactar en la imagen de la ADR. ▪ Fallas en la operación por la identificación tardía de incidentes repetitivos y/o sin solución pertinente.

Recomendación(es):

- Definir lineamientos para el correcto y completo registro de los casos reportados en la mesa de servicio y garantizar que se pueda realizar la trazabilidad de todos los casos, contando con la evidencia completa y suficiente.

- Identificar si una capacitación formal del uso de la herramienta y de los lineamientos propuestos por ITIL[8] (Biblioteca de Infraestructura de Tecnologías de Información - ITIL, por sus siglas en inglés) para la prestación del servicio apoyarían la gestión realizada por los funcionarios que atienden la mesa de ayuda.

- Unificar los criterios a registrar en la herramienta de gestión de incidencias, en cuanto a la clasificación, categorización y priorización del problema, que permitan poblar eficientemente todos los atributos contemplados en la herramienta. Una buena mesa de ayuda es fundamental para que la gestión de incidentes funcione eficientemente, por lo cual, se deberá incluir un control de seguimiento documentado del proceso.

[8] Conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. Tomado de https://www.axelos.com/best-practice-solutions/itil

- Definir e implementar métricas que permitan determinar el número y gravedad del incidente reportado, para realizar un análisis de los más críticos con los soportes de solución y así poder determinar si este es repetitivo o aislado, de tal manera que, permita tomar las medidas pertinentes.

Algunas métricas sugeridas por las buenas prácticas establecidas en el Modelo COBIT 2019, están:

- Porcentaje de problemas identificados correctamente, incluida la clasificación, categorización y priorización de estos.
- Porcentaje de incidentes resueltos conforme a los Niveles de Servicio Acordados (SLA, por sus siglas en inglés).
- Incidentes recurrentes causados por problemas no resueltos.
- Porcentaje de soluciones temporales definidas para los problemas abiertos.

Respuesta del Auditado: Aceptado Parcialmente.

Justificación: "*Si bien no se objetan los hallazgos, dejamos claro que no estamos de acuerdo con la descripción de los Riesgos y con la descripción de los Impactos, teniendo en cuenta que, no hay una relación directa entre la documentación de casos de soporte y los riesgos. Es claro que las actividades de documentación se ejecutan en un sistema diferente (Aranda) y no hay una relación directa entre lo observado y los riesgos:*

- *Fallas tecnológicas en el aplicativo Banco de Proyectos y/o en la infraestructura técnica (hardware, redes y comunicaciones) que lo soporta, que afecta la seguridad de la información.*
- *Errores en la ejecución de procesos que impidan la disponibilidad de la información.*

- *Falla en la operatividad en el aplicativo Banco de Proyecto, para el módulo de Proyectos, Evaluación y Calificación.*

Adicionalmente encontramos que no hay relación directa entre lo observado y los impactos, en especial sobre el concepto de "facilitar la realización de fraude" que es algo muy grave. Sobre los impactos:

- *Errores o incidentes que afecten la recuperación y seguridad de la información.*
- *Indisponibilidad del servicio para un proceso misional debido a errores repetitivos no solucionados de raíz.*
- *El acceso a información sensible puede facilitar la realización de fraude e impactar en la imagen de la ADR.*"

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Imposibilidad de realizar trazabilidad a los incidentes reportados en la mesa de servicio.
- Falta de definición de lineamiento para el correcto registro (tipificación, definición de impacto, urgencia, prioridad, nombre del SLA, entre otros) de los incidentes en la mesa de servicio.
- Desconocimiento de las bondades que ofrece la herramienta.
- Ausencia de un repositorio centralizado para el almacenamiento de evidencias de los incidentes reportados.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Plan de mejora del servicio que incluye capacitación a los agentes, definición de métricas sobre la trazabilidad de los casos	1 Plan ejecutado	Correctiva	Equipo Humano OTI	1-nov-2020	31-dic-2020
Socialización de métricas para el número y gravedad del incidente	1 socialización de indicadores	Correctiva	Equipo Humano OTI	1-nov-2020	31-dic-2020
Creación y puesta en producción de un repositorio centralizado para el almacenamiento de evidencias de los incidentes reportados.	1 repositorio en operación	Correctiva	Equipo Humano OTI	1-nov-2020	31-dic-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Analizado el plan de mejoramiento propuesto por los responsables de la unidad auditada, la Oficina de Control Interno lo acepta en razón a que las acciones de mejoramiento establecidas guardan correspondencia con las causas determinadas para este hallazgo, y la OTI acepta el hallazgo; no obstante, en cuanto a sus observaciones sobre riesgo e impactos, se precisa que, los riesgos e impactos identificados por la Oficina de Control Interno corresponden a lo evidenciado en la auditoría, puesto que no se pudo obtener trazabilidad de la atención y solución completa de los casos reportados en ARANDA, iniciando por una correcta tipificación de éstos.

Al respecto, las buenas prácticas del Marco ITIL. COBIT 2019 y la Norma ISO 27001:2013, indican que "*El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros*" (Anexo A.16.1.6.) y que "*La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia*". (Anexo A.16.1.7.)

Aranda, es una herramienta valiosa que, si bien se utiliza para registrar los casos reportados, se convierte a su vez en una base de conocimiento que bien administrada

provee información para la atención de casos reiterativos, por ello, contar con una inadecuada o insuficiente información sobre casos previos puede repercutir aplicar correctivos que no contienen información o pasos completos para la solución, ocasionando posibles fallas tecnológicas o demoras en la solución de éstas, así como posibles errores en la ejecución de procesos que impidan la disponibilidad de la información.

HALLAZGO N° 8. Ausencia de procedimientos para la gestión de logs y registros de auditoria de actividades realizadas por los usuarios.

Descripción: La Oficina de Control Interno evidenció que el aplicativo Banco de Proyectos cuenta con una serie de logs activos de autoría predefinidos, a los cuales se accede por el módulo de configuración; sin embargo, dentro de los logs almacenados no es posible determinar las acciones y actividades que está registrando, evidenciando que la administración del sistema no tiene un claro conocimiento de la información que se está generando como rastro de auditoría, tanto a nivel de consulta como de la estructura e interpretación de los registros.

Adicionalmente, se pudo evidenciar que:

- No se tienen identificadas y definidas las actividades críticas que deban ser monitoreadas en el sistema.
- No se identifican informes de errores y excepciones.
- No se realiza monitoreo sobre los logs que están activos.
- No se identifica un responsable del monitoreo.

De acuerdo con lo establecido en la norma ISO 27001:2013, **numeral A12.4 "*Registro y Seguimiento"*** que tiene como objetivo registrar los eventos dentro del sistema y generar evidencia, se determinan los siguientes controles para garantizar la trazabilidad de los eventos dentro de los sistemas de información:

- "***A12.4.1. Registro de eventos***. *Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.*

- ***A12.4.2. Protección de la información de registro***. *Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.*

- ***A12.4.3. Registros del administrador y del operador***. *Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad*."

No obstante lo anterior, no se evidenció que la Agencia contara con un documento formal que contenga los lineamientos para asegurar la trazabilidad de los eventos en el sistema de información.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Ausencia de un procedimiento para la gestión de logs de autoría. ▪ Desconocimiento de la estructura de los logs que son registrados en el sistema de Banco de Proyectos. ▪ Falta de definición de actividades críticas en el sistema de Banco de Proyectos. ▪ Falta de personal que realice la actividad de monitoreo y sea independiente a los usuarios administradores del sistema.	▪ Acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos ▪ Errores en la ejecución de procesos que impidan la disponibilidad de la información. ▪ Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero.	▪ Imposibilidad para identificar el responsable de actividades no autorizadas dentro del sistema por ausencia de logs. ▪ Identificación tardía de actividades no autorizadas dentro del sistema.

Recomendación(es): Debido a que a la fecha de la auditoría (30 de septiembre de 2020) la Agencia no tenía contrato de soporte con el proveedor que desarrolló el aplicativo Banco de Proyectos, es importante evaluar la posibilidad de buscar el acompañamiento del proveedor para tener una capacitación sobre la estructura, interpretación y construcción de logs, bien sea bajo la modalidad de bolsa de horas o con un contrato de

asesoría, de tal forma que, le permita a la ADR diseñar y formalizar un procedimiento para la gestión de logs y registro de auditoria, donde se definan entre otras cosas:

- **Actividades críticas**. Se deben definir los eventos a registrar por cada sistema tales como:
  - Cambio de Estado de Formulario.
  - Recuperación de Archivos Adjuntos.
  - Intentos de acceso exitosos y fallidos.
  - Desconexiones del sistema.
  - Acciones ejecutadas.
  - Alertas por fallos en el sistema.
  - Fecha y hora en que se producen los eventos.
  - Tiempos de detención.
- **Estructura**. Se debe determinar la información y estructura que debe tener cada uno de los registros a almacenar, como fecha, hora, usuario, IP de conexión, actividad realizada, entre otros.
  - **Monitoreo**. Revisar los registros de forma periódica, independientemente de si hay un incidente o no permite analizar tendencias, detectar potenciales actividades fraudulentas, o detectar el origen de fallos de funcionamiento, antes de que ocurran incidentes importantes. Se debe definir la periodicidad de monitoreo, responsable y evidencias de revisión.
  - **Protección de los registros de auditoria**. Los registros de eventos deben tener el nivel de protección apropiado para evitar pérdidas, corrupción o cambios no

autorizados. El administrador del sistema no debe tener permiso para borrar o desactivar el registro de sus propias actividades. Se deben guardar copias de seguridad de los registros de eventos.

- **Logs de usuarios administradores**. Registrar las actividades de los usuarios administradores, teniendo especial cuidado con los que tienen privilegios de administración dado el riesgo que tiene si pueden acceder a los registros y manipularlos o borrarlos.

Respuesta del Auditado: Aceptado.

Justificación: "*La ausencia de un procedimiento para la gestión de logs de auditoría, el desconocimiento de la estructura de los logs que son registrados en el sistema de Banco de Proyectos, debido a una falta de previsión en la necesidad de hacer este tipo de revisiones; la falta de definición de actividades críticas en el sistema de Banco de Proyectos, y por ende, el no estar definido qué personal realice la actividad de monitoreo, y sea independiente a los usuarios administradores del sistema, propiciaron los hallazgos encontrados, por lo que, el plan de mejoramiento expuesto busca avanzar en un mayor nivel de madurez que permita contemplar estos riesgos que pueden afectar la operatividad y seguridad del sistema de Banco de Proyectos.*"

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Ausencia de un procedimiento para la gestión de logs de autoría.
- Desconocimiento de la estructura de los logs que son registrados en el sistema de Banco de Proyectos.
- Falta de definición de actividades críticas en el sistema de Banco de Proyectos.
- Falta de personal que realice la actividad de monitoreo y sea independiente a los usuarios administradores del sistema.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Elaborar, aprobar, institucionalizar, socializar (a quien corresponda) un procedimiento para el control del registro, conservación y revisión regular de los registros de eventos (logs) acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Institucionalización del procedimiento para el control del registro, conservación y revisión de logs del sistema de Banco de Proyectos	Correctiva	Equipo Humano OTI	01-nov-2020	28-feb-2021
Realización de capacitación en la administración del sistema de Banco de Proyectos (funcionalidad, arquitectura, seguridad, bases de datos, mecanismos de interoperabilidad) con el proveedor del sistema PricewaterhouseCoopers	Sesiones de capacitación realizadas	Correctiva	Equipo Humano OTI	01-nov-2020	30-dic-2020
Descripción de las actividades críticas del sistema Banco de Proyectos presente en la definición del procedimiento de gestión del Banco de Proyectos.	Definición de actividades críticas en el sistema de Banco de Proyectos.	Correctiva	Equipo Humano OTI	01-nov-2020	31-oct-2020
Actualización del documento de procedimiento de gestión del Banco de Proyectos incluyendo roles respecto al monitoreo.	Definición de responsabilidades respecto a la gestión del sistema Banco de Proyectos	Correctiva	Equipo Humano Vicepresi-dencia de Proyectos	19-oct-2020	30-nov-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) y de la Vicepresidencia de Proyectos responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado.

Analizado el plan de mejoramiento propuesto por los responsables de la unidad auditada, la Oficina de Control Interno lo acepta considerando que da cobertura a las causas principales identificadas para este hallazgo.

HALLAZGO N° 9. Inadecuada gestión y monitoreo de mecanismos de recuperación en caso de contingencia.

Descripción: Acorde con la información suministrada a la Oficina de Control Interno, en relación con la programación, almacenamiento y restauración de copias de respaldo del aplicativo Banco de Proyectos en los dos escenarios aplicables al período auditado, servidores on-premise (1 servidor físico con tres máquinas virtualizadas) y el actual en la nube (manteniendo el mismo esquema), se efectuó revisión del cumplimiento del procedimiento "Generación y Administración de copias de seguridad de las Bases de Datos" (DE-GTI-003), en lo que no se identificó lineamientos internos para los servidores del aplicativo Banco de Proyectos.

Si bien la programación de los backups se realiza una única vez para que en adelante se ejecuten las copias de respaldo de manera automática, la ADR ha definido acciones que soportan estas actividades de control y que deben ser realizadas por parte del Administrador de la Base de Datos (DBA, por sus siglas en inglés) como es el caso del registro de la *"Planilla de generación de respaldo de bases de datos"* (formato DE-GTI-004) versión 3.

Teniendo en cuenta que esta actividad de control (Backups) tiene una frecuencia diaria, para el período auditado se seleccionó una muestra de 40 fechas (días) en las cuales se debía realizar la copia de respaldo, tanto para la base de datos como para los servidores, así:

SERVIDORES VIRTUALES EN EL DATACENTER *Esquema Anterior*		**SERVIDORES VIRTUALES EN LA NUBE** *Esquema Actual a partir del 24-jul-2020*	
SRVBANPROYECTO01 - E:\SRVBANPROYAPP01	6	SRVBANPROYECTO01 - E:\SRVBANPROYAPP01	1
SRVBANPROYECTO01 - E:\SRVBANPROYWFE01	5	SRVBANPROYECTO01 - E:\SRVBANPROYWFE01	1
SRVBANPROYECTO01 - D:\SRVBANPROYSQL01	8	SRVBANPROYECTO01 - D:\SRVBANPROYSQL01	1

SERVIDORES VIRTUALES EN EL DATACENTER *Esquema Anterior*		SERVIDORES VIRTUALES EN LA NUBE *Esquema Actual a partir del 24-jul-2020*	
Base de Datos SRVBANPROYSQL01	16	Base de Datos SRVBANPROYSQL01	2
CANTIDAD TOTAL SELECCIONADA	**35**	**CANTIDAD TOTAL SELECCIONADA**	**5**

Con base en las muestras seleccionadas, la Oficina de Tecnologías de la información proporcionó únicamente las "*Planillas de generación de respaldo de bases de datos*" (DE-GTI-004) de los meses de agosto a diciembre de 2019, de las cuales, la Oficina de Control Interno evidenció diligenciadas 5 de las 18 fechas requeridas de esos períodos, sin obtener adicionalmente evidencia de los logs de finalización que permitieran identificar el estado de terminación (exitoso o con error).

Para el caso de servidores, no se identificó un lineamiento para la realización de las copias (esto aplicable hasta cuando se tuvo el servidor y las máquinas virtualizadas del aplicativo Banco de Proyectos en las instalaciones de la ADR).

Para la muestra seleccionada de servidores, el Ingeniero a cargo de la administración de Infraestructura Tecnológica proporcionó evidencia para 5 de las 22 fechas requeridas, en un formato no codificado denominado "*Bitácora de Almacenamiento*" el cual contenía: *"ID, Nombre de la Copia, Nombre de quien realiza la copia, Fecha de realización, Ubicación, ¿Backup exitoso? (Caso contrario realizar observaciones)*".

No se obtuvo evidencia de los logs de finalización que permitieran identificar el estado de terminación frente a lo reportado. Al respecto, la OTI informó en correo electrónico del 17 de septiembre de 2020 […] "*las copias de seguridad de las máquinas que soportan la aplicación, tal como se escribe en el documento: Debido a lo básica que es la herramienta de generación de backups no es posible obtener los logs y registros solicitados"*.

Al 30 de septiembre de 2020 se mantenía el mismo esquema de respaldo para los servidores que se migraron a finales de julio de 2020 a la nube con Microsoft Azure,

siendo la ADR el responsable de la ejecución de este control; al respecto, no se obtuvo evidencia del monitoreo para las fechas seleccionadas en la muestra.

Por otra parte, de acuerdo con lo establecido en el procedimiento "Generación y Administración de copias de seguridad de las Bases de Datos" (DE-GTI-003), el cual indica en su numeral "*5.7. Verificar la consistencia del respaldo. Realizar una verificación aleatoria de tres bases de datos en el semestre de cada servidor de base de datos que se encuentre bajo la administración de la Oficina de Tecnologías de la Información*", sólo se recibió el último reporte de restauración de copias de respaldo que correspondía al 29 de agosto de 2019, y sobre el cual no fue suministrada la documentación soporte de la ejecución del control y el resultado de la restauración. De acuerdo con lo indicado por los Ingenieros de la OTI, la no ejecución de este control estaba asociada a la ausencia del DBA, quien tiene a cargo esta actividad de manera trimestral.

Finalmente, en cuanto al Plan de Contingencia Tecnológico para el aplicativo Banco de Proyectos, la OTI proporcionó el documento "Plan de Contingencia - Banco de Proyectos" con fecha 31 de octubre de 2017, primera versión para discusión. Resultado de su revisión, se identificó que:

- Este documento fue preparado por el proveedor con el propósito de […] "*presentar a la Agencia de Desarrollo Rural el plan de contingencia de la solución de proyectos, antes de la salida a producción y solo para los artefactos tecnológicos propios y directos del sistema, es decir, no contempla las variables que son administradas directamente por la Agencia de Desarrollo Rural, ya que la solución debe ser incorporada en los planes de continuidad de negocio que tenga la entidad*."

- Durante el período auditado, no se realizaron pruebas al Plan de Contingencias para el aplicativo Banco de Proyectos, ni antes ni posterior a la puesta en producción de la versión 2 del aplicativo, y de la migración de los servidores a la nube. Al 30 de septiembre de 2020 se desconocía la aplicabilidad y vigencia del documento proporcionado por el proveedor.

Además, en el Sistema Integrado de Gestión (aplicativo ISOLUCIÓN) se observó el documento "Plan de Contingencia para Riesgos Materializados GTI" (PDC-GTI-001), versión 1 publicado el 26 de junio de 2018, en el cual se enumeran las acciones a realizar para dar manejo a la materialización del riesgo de Pérdida o daño de información. Una vez revisado el documento, se identificó que su contenido corresponde a un manejo de incidentes.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ No se cuenta con un profesional especializado para realizar las gestiones de Administración de Bases de Datos (DBA) desde el mes de diciembre de 2019. ▪ Insuficiencia de recurso humano en la Oficina de Tecnologías con las competencias técnicas requeridas para realizar la administración y gestión de las copias a nivel de bases de datos. ▪ Ausencia de lineamientos formales para la gestión y monitoreo de mecanismos de recuperación en caso de contingencia (copias de respaldo, restauración, pruebas al plan de contingencia tecnológico del aplicativo).	▪ Incumplimiento legal de normas/leyes internas y externas aplicables a los procesos de ADR. ▪ Fallas tecnológicas en el aplicativo Banco de Proyectos y/o en la infraestructura técnica (hardware, redes y comunicaciones) que lo soporta, que afecta la seguridad de la información. ▪ Errores en la ejecución de procesos que impidan la disponibilidad de la información. ▪ Falla en la operatividad en el aplicativo Banco de Proyecto, para el módulo de Proyectos, Evaluación y Calificación. ▪ Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero.	▪ Errores o incidentes que afecten la recuperación y seguridad de la información. ▪ Indisponibilidad del servicio para un proceso misional debido a errores en la ejecución de tareas programadas, o en caso de una interrupción significativa. ▪ El acceso a información sensible puede facilitar la realización de fraude e impactar en la imagen de la ADR.

Recomendación(es):

- Capacitar o contratar un funcionario entrenado para desempeñar el cargo de Administrador de Bases de Datos (DBA), contando así con el personal técnico requerido para la administración y gestión de las bases de datos de la ADR, teniendo como premisa que la gestión del conocimiento técnico minimiza la exposición de la Agencia a dependencias críticas sobre individuos clave de la Oficina de Tecnologías de la información.

- Asegurar que para todas las copias de respaldo de la base de datos del aplicativo Banco de Proyectos se sigan los lineamientos y se cumplan los requisitos definidos en el procedimiento “Generación y Administración de copias de seguridad de las bases de datos” (DE-GTI-003), garantizando que se verifica y se registra la ubicación y estado de finalización de la copia de datos de acuerdo con la programación.

- Revisar y ajustar la “Planilla de generación de respaldo de las bases de datos” (DE-GTI-004), de tal forma que incluya el funcionario responsable, así como el estado de finalización del respaldo, y las acciones tomadas en caso de presentarse inconsistencias.

- Teniendo en cuenta que la responsabilidad de programar y realizar monitoreo de las copias de respaldo de los servidores ahora en la nube continúa siendo de la ADR, se requiere dejar registro específico por parte del supervisor del contrato, de los controles de monitoreo establecidos para garantizar la correcta toma y restauración de las copias de respaldo.

- Definir e implementar un lineamiento que establezca que, para la aplicación Banco de Proyectos se realizará al menos dos veces al año la restauración de copias de respaldo, dejando soporte de los pasos que conlleva el desarrollo de la prueba, así como de los resultados obtenidos y acciones tomadas en caso de error, esto, con el fin de verificar que los medios de respaldo funcionan correctamente y que siguiendo el procedimiento establecido se logra su restauración. Adicionalmente, el reporte (planilla o formato que se establezca), deberá ser firmado por la persona que realizó la restauración.

- Revisar la validez y aplicabilidad del documento provisto por el proveedor del aplicativo, en relación con el Plan de Contingencia Tecnológico para el aplicativo Banco de Proyectos, considerando el entorno actual y versión en la que se encuentra el aplicativo, de tal forma que en caso de una eventualidad y/o interferencia en las operaciones del proceso misional que se lleva en el aplicativo, le permita a la OTI

atender la contingencia y retornar a la operación normal en poco tiempo y con un bajo impacto económico.

Para ello, es necesario verificar si el documento del año 2017 da cumplimiento a los elementos mínimos de un Plan de Contingencia, tales como:

a. Resultado del análisis de riesgos.

b. Análisis de impacto.

c. Procedimientos de activación, recuperación y retorno a operación normal.

d. Definición de las estrategias para atender la contingencia.

e. Referencia a los planes de recuperación establecidos para el aplicativo y la plataforma que lo soporta.

f. Directorios de contacto y árboles de llamada del equipo de recuperación del proceso.

g. Actividades administrativas a ejecutar durante operación normal para mantener el plan operativo y actualizado. Así, como los lineamientos para realizar la documentación propia de plan, pruebas, capacitaciones, actualización y mejora continua del Plan de Contingencia.

- Actualizar el análisis de riesgos e impacto de los procesos de TI y los planes de recuperación de la infraestructura para el aplicativo Banco de Proyectos. Acorde con lo recomendado por las buenas prácticas, esto debe realizarse de forma periódica (Anual), al igual que se debe hacer con el Plan de Contingencia.

Respuesta del Auditado: Aceptado Parcialmente.

Justificación: "*Dentro del Talento Humano que se tenía definido en el PETI se involucraba la contratación de un DBA, el cual no se pudo contratar debido a las*

restricciones que se presentaron en la contratación y no se encontraba una persona que cumpliera con el perfil requerido para ejecutar las actividades que se necesitaban en la Entidad. A partir del mes de octubre se logró contratar un Ingeniero con el perfil requerido para la Administración de Bases de Datos, quien se encuentra en este momento identificando y apropiándose de las diferentes Bases de Datos que se tienen en la Entidad, por lo anterior, se acepta parcialmente el hallazgo.

Respecto al procedimiento de Backups, ya se ha elaborado una versión preliminar que se encuentra en espera de aprobación para su cargue al Sistema Integrado de Gestión (aplicativo ISOLUCION)."

Causa(s) identificada(s) por el Responsable de la Unidad Auditada: Ausencia de lineamientos formales para la gestión y monitoreo de mecanismos de recuperación en caso de contingencia (copias de respaldo, restauración, pruebas al plan de contingencia tecnológico del aplicativo).

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Elaborar el procedimiento de Administración de Copias de Respaldo Backup con el objetivo de establecer soluciones tecnológicas seguras y oportunas para que los servicios y recursos de TI se vean respaldados por un procedimiento de Backups.	Realizar el procedimiento de Administración de Copias de Respaldo Backup	Correctiva	Equipo Humano OTI	20-oct-2020	20-nov-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Analizado el plan de mejoramiento propuesto por los responsables de la unidad auditada, la Oficina de Control Interno lo acepta considerando que da cobertura a la causa identificada; sin embargo, en el análisis de los argumentos expuestos en la justificación, la Oficina de Control Interno no identificó los elementos con los cuales se demuestre que

se cumplió parcialmente. Para el periodo auditado, no se contó con un DBA desde mediados del mes de diciembre de 2019, el período restante fue suplido por otros funcionarios de la OTI quienes propendieron por atender las situaciones que se pudieran presentar. Adicionalmente, no se evidenció documentación soporte y formal de las actividades realizadas, y la OTI no contó con el perfil técnico requerido para el cargo, de lo cual, la OCI no obtuvo evidencia, tal como se reportó en el hallazgo.

Por otra parte, es pertinente indicar respecto a las deficiencias que no fueron tenidas en cuenta para la inclusión de acciones preventivas o correctiva en el plan de mejoramiento, que la OTI deberá revisar e incluir para su análisis y ajuste, los siguientes aspectos:

- Revisar la validez y aplicabilidad del documento provisto por el proveedor del aplicativo, en relación con el Plan de Contingencia Tecnológico para el aplicativo Banco de Proyectos, considerando el entorno actual y versión en la que se encuentra el aplicativo.

- Actualizar el análisis de riesgos e impacto de los procesos de TI y los planes de recuperación de la infraestructura para el aplicativo Banco de Proyectos.

HALLAZGO N° 10. Ausencia de lineamientos para el monitoreo de capacidad y disponibilidad de la infraestructura tecnológica hardware y software para Banco de Proyectos.

Descripción: En cuando a la **Seguridad de las Operaciones** el numeral 6.6. de la Guía N° 3 “Procedimientos de Seguridad de la información” del MinTIC, señala “*Procedimientos de Gestión de Capacidad”*, indicando que: “*Se debe especificar como la organización realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son escasos, demorados en su arribo o costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda, etc*.”

Así mismo, los anexos A.12.1.1 “*Procedimientos de operación documentados*” y A.12.1.3 “*Gestión de capacidad*” de la Norma ISO 27001:2013, indican que:

- A.12.1.1. "*Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.*"

- A.12.1.3. "*Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.*"

Considerando la normativa anterior, en las verificaciones realizadas por la Oficina de Control Interno se evidenció:

a. A la fecha de corte del período auditado (31 de julio de 2020) la ADR no contaba con un procedimiento formalizado y divulgado para la gestión de la capacidad y disponibilidad de los servidores y las bases de datos. Al 30 de septiembre de 2020 el monitoreo estaba a cargo del Administrador de Infraestructura para servidores y bases de datos, teniendo en cuenta que a la fecha de corte no se contaba con un DBA - Administrador de Base de Datos.

b. En la verificación del procedimiento "Administración de Redes" (PR-GTI-005) aprobado el 7 de julio de 2020, y que tiene por objetivo "*Realizar el soporte y actualización de las redes de cómputo para agilizar los procesos administrativos en la operación de los servicios de red que proporciona la ADR, garantizándole al personal un fácil acceso a los aplicativos y servicios como correo electrónico, Internet, bases de datos, entre otros*", se identificó que la OTI realiza un monitoreo constante de la disponibilidad de la infraestructura tecnológica a través de la herramienta *Nagios*.

   Se requirieron los documentos soporte de monitoreo de alertas generadas de las revisiones a la red, al Firewall, y al Switch core, observando que solo se cuenta con el reporte mensual "Informe de Gestión" que consolida entre otros temas, el global de los incidentes y requerimientos reportados en la mesa de servicios (ARANDA).

c. En el manual "Arquitectura Banco de Proyectos" versión 1.0 del 18 de enero 2020, entregado a la ADR por el proveedor de la solución, se detalla la arquitectura del Banco de Proyectos en sus capas de Datos y de Negocio. No se obtuvo evidencia de la documentación de líneas base de configuración que incluyeran las descripciones y

relaciones entre los recursos clave y las capacidades necesarias para ofrecer el servicio que depende de la infraestructura del Banco de Proyectos.

d. No se tuvo conocimiento que la ADR cuente con líneas de referencia y criterios de atención de alertas para la disponibilidad, capacidad y rendimiento de la infraestructura tecnológica que soporta el aplicativo Banco de Proyectos, que permita realizar comparaciones contra los niveles actuales de utilización, capacidad disponible y rendimiento de los equipos y las bases de datos (mediante la generación de estadísticas). La documentación de las líneas de referencia es importante para no dejar el análisis de disponibilidad, capacidad y rendimiento a criterio de las personas que lo ejecutan.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Ausencia de un procedimiento para la gestión de la capacidad y disponibilidad de la infraestructura. ▪ Confianza en la capacidad de almacenamiento en la nube con Microsoft AZURE ▪ Falta de anticipación en dimensionamiento de recursos de infraestructura críticos en el sistema de Banco de Proyectos.	▪ Incumplimiento legal de normas/leyes internas y externas aplicables a los procesos de ADR. ▪ Acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos. ▪ Fallas tecnológicas en el aplicativo Banco de Proyectos y/o en la infraestructura técnica (hardware, redes y comunicaciones) que lo soporta, que afecta la seguridad de la información. ▪ Errores en la ejecución de procesos que impidan la disponibilidad de la información. ▪ Falla en la operatividad en el aplicativo Banco de Proyecto, para el módulo de Proyectos, Evaluación y Calificación. ▪ Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero.	▪ Afectación de la disponibilidad del servicio, mejorando la eficiencia en la gestión de recursos y optimizar el desempeño de los sistemas anticipando los requerimientos de capacidad mediante predicciones del desempeño futuro. ▪ Incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público. ▪ Identificación tardía de actividades claves para la disponibilidad de la infraestructura. ▪ Errores o incidentes que afecten la recuperación y seguridad de la información. ▪ Indisponibilidad del servicio para un proceso misional debido a que no se proyecte el crecimiento o necesidad de recursos tecnológicos. ▪ El acceso a información sensible puede facilitar la realización de fraude e impactar en la imagen de la ADR.

Recomendación(es): Tal como lo propone la Guía 3 del MinTIC en la sección 6.6. Seguridad de las Operaciones, la ADR debe establecer un procedimiento de gestión de la capacidad para los sistemas de información críticos, el cual incluye el Banco de Proyectos, y en detalle los anexos A.12.1.1 "*Procedimientos de operación documentados*" y A.12.1.3 "*Gestión de capacidad*" de la Norma ISO 27001:2013; para ello se deben considerar los siguientes aspectos:

- Identificar y documentar las líneas base de configuración del servidor(es) de Banco de Proyectos y de la base de datos
- Definir y formalizar las líneas de referencia de disponibilidad, capacidad y rendimiento de la infraestructura tecnológica.
- Definir, formalizar e implementar un procedimiento para la generación de informes con las estadísticas y tendencias sobre la capacidad y disponibilidad de la infraestructura de TI que soporta el Banco de Proyectos, en el cual se incluya aspectos como:
  - Responsables de las actividades
  - Actividades para generar estadísticas y tendencias en el informe
  - Actividades para la revisión de las tendencias por parte del personal adecuado, en la cual se definan planes de acción y se definan nuevos requerimientos en caso de necesitarlos.

  Algunas métricas que se pueden implementar son:

  - Número de eventos que exceden los límites de capacidad planificados
  - Número de picos de transacciones que exceden el rendimiento objetivo
  - Porcentajes de uso real de la capacidad, Porcentaje de disponibilidad real y Porcentaje de rendimiento real

El análisis de estadísticas y tendencias es parte del monitoreo, detección e implementación de mejoras en el desempeño de bases de datos, sistemas operativos y software de aplicación.

Respuesta del Auditado: Aceptado Parcialmente.

Justificación: "*La Oficina de Tecnologías de la Información en el presente año, con relación a los procesos que apalancan la operación y el soporte de infraestructura, identificó la necesidad de documentar y definir la gestión de la capacidad de TI, con el objetivo de toma de decisiones estratégicas basado en un plan de capacidad para la administración de la infraestructura que soporta los servicios tecnológicos de la Agencia.*

La OTI cuenta con el almacenamiento en la nube por medio de Microsoft Azure, con este tipo de contratación la gestión de la capacidad se realiza a través del tercero y la ADR hace un constante monitoreo de la gestión de los créditos con un profesional especializado como administrador de la infraestructura. Actualmente, se viene desarrollando la adquisición de nuevos créditos que dan continuidad al servicio, se han realizado sesiones de trabajo con el proveedor de la herramienta (Microsoft) con el fin de implementar las mejores prácticas que ofrece Azure, no solo a nivel de almacenamiento sino también para la operación y transaccionalidad que con los diversos sistemas (no solo banco de proyectos) y bases de datos que operan en la nube."

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Ausencia de lineamientos que defina un plan de capacidad, el cual genera fallas de operatividad del Banco de Proyectos.
- Ausencia de un procedimiento que describa los pasos para la gestión de capacidad para los servicios tecnológicos.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Generar los lineamientos que definan las variables y los elementos a tener en cuenta para el plan de capacidad del banco de proyectos.	Realizar el plan de capacidad	Correctiva	Equipo Humano OTI	20-oct-2020	01-mar-2021
Elaborar el procedimiento con el objetivo de establecer soluciones tecnológicas seguras y oportunas para que los servicios y recursos de TI se vean respaldados por una capacidad de procesamiento y almacenamiento suficiente y correctamente dimensionado.	Realizar procedimiento para la gestión de la capacidad de los servicios tecnológicos	Preventiva	Equipo Humano OTI	20-oct-2020	30-nov-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Analizado el plan de mejoramiento propuesto por los responsables de la unidad auditada, la Oficina de Control Interno lo acepta considerando que da cobertura a las causas principales identificadas, bajo el entendido de que al momento de realizar la acción "*Generar los lineamientos que definan las variables y los elementos a tener en cuenta para el plan de capacidad del Banco de Proyectos*" tendiente a "*Realizar el plan de capacidad*" se tomarán como base las identificaciones y documentaciones previas de las líneas base de configuración del servidor(es) de Banco de Proyectos y de la base de datos.

HALLAZGO N° 11. Inobservancia del desarrollo de pruebas de vulnerabilidad al Banco de Proyectos y su entorno.

Descripción: De acuerdo con lo establecido en la Norma ISO 27001:2013, numeral A12.6 el cual hace referencia a la "Gestión de la Vulnerabilidad Técnica", cuyo objetivo es prevenir el aprovechamiento de las vulnerabilidades técnicas, indica […] "*se deberían tomar acciones apropiadas y oportunas en respuesta a la identificación de*

vulnerabilidades técnicas potenciales", la Oficina de Control Interno validó el desarrollo y gestión de pruebas de vulnerabilidad.

Si bien la Oficina de Tecnologías de la Información (OTI) tiene el compromiso definido en el MSPI, relacionado con "*Definir lineamientos para ejecutar las pruebas de vulnerabilidades*", se conoció que en el mes de abril de 2020 la OTI realizó pruebas de vulnerabilidad al aplicativo Banco de Proyectos haciendo uso de la herramienta OWASP ZAP 2.8.0.[9]. Así mismo, se tuvo acceso al informe de resultados, sobre el cual se identificaron las siguientes situaciones:

- El Informe presentado corresponde únicamente a un escaneo realizado al aplicativo Banco de Proyectos con el fin de identificar vulnerabilidades; en éste, se registraron las alertas y posibles soluciones que la misma herramienta genera, sin contar con un análisis técnico por parte del ejecutor del control, que le permitiera a la ADR establecer los impactos internos e identificar falsos positivos.

- La actividad realizada está incompleta y no cumple con el objetivo que propone un ejercicio de pruebas de vulnerabilidad, y lo que conlleva analizar el entorno que soporta el aplicativo Banco de Proyectos, el cual arrojaría como resultado, luego de cumplir las fases requeridas en una prueba de vulnerabilidades, contar con una evaluación completa y objetiva de los componentes que deberían haber sido considerados.

- No se incluyó la gestión de las vulnerabilidades identificadas, mediante la generación del plan de acción y la mitigación de riesgos.

- El indicador establecido se encontraba en 0%

- Al 31 de agosto de 2020 el documento puede no estar vigente para la formulación de planes de acción, teniendo en cuenta los cambios que se han presentado en lo corrido

[9] Herramienta de uso gratuito disponible en Internet

del año con la puesta en producción de la versión 2 del aplicativo Banco de Proyectos, y la migración de las máquinas virtuales a la nube a finales del mes de julio de 2020.

- No se identificó la fecha de realización del escaneo, ni a quién va dirigido el reporte.
- No se identificó una periodicidad definida para realizar pruebas de vulnerabilidad.

De otra parte, en la revisión del contrato suscrito para el desarrollo e implementación de las versiones 1 y 2 del aplicativo Banco de Proyectos, no se identificaron cláusulas donde se le requiera al proveedor de la solución realizar pruebas de vulnerabilidad como parte del aseguramiento de la solución.

Adicionalmente, se conoció que para el periodo auditado no se realizaron pruebas de seguridad perimetral, las cuales son necesarias, toda vez que, el aplicativo Banco de Proyectos se encuentra público en internet, y para su acceso se dispone de dispositivos que apoyan su seguridad y restricción de acceso que deben ser evaluados periódicamente.

Además, no se encontró evidencia de algún procedimiento para la gestión de vulnerabilidades, por lo que la Oficina de Control Interno no pudo concluir sobre:

- Generación de reportes de conclusiones que contengan de manera priorizada las vulnerabilidades críticas identificadas y su nivel de riesgo, de acuerdo con el análisis efectuado.
- Ejecución y monitoreo de las correcciones que sean necesarias sobre las debilidades identificadas, a través de la aplicación de parches, controles o actualizaciones a las que haya lugar.
- Verificación de que las vulnerabilidades identificadas fueron solucionadas y no son reportadas en el nuevo escaneo realizado.

Finalmente, al 31 de agosto de 2020 no se identificó en el mapa de riesgos vigente del proceso Gestión de Tecnologías de la Información (GTI) la inclusión de riesgos asociados a Seguridad de la Información y Ciberseguridad.

Posible(s) Causa(s), Riesgo(s) e Impacto(s):

CAUSA(S)	RIESGO(S)	IMPACTO(S)
▪ Ausencia de una metodología clara en la ejecución de las pruebas de vulnerabilidades y en su interpretación. ▪ Discrecionalidad en la ejecución de los controles ejecutados a discreción por el dueño del proceso. ▪ Dependencia del conocimiento técnico del responsable de la ejecución del control.	▪ Fallas tecnológicas en el aplicativo Banco de Proyectos y/o en la infraestructura técnica (hardware, redes y comunicaciones) que lo soporta, que afecta la seguridad de la información. ▪ Acceso a información o cambios no autorizados en el aplicativo Banco de Proyectos ▪ Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero. ▪ Dependencia del conocimiento del Profesional que ejecuta el control, por ausencia de documentación necesaria para su desarrollo y gestión.	▪ Indisponibilidad del servicio al presentarse fallas que no son identificadas o gestionadas de manera oportuna. ▪ Explotación de vulnerabilidades impactando los pilares de la seguridad de la información. ▪ Identificación de eventos de seguridad basados únicamente en un componente de seguridad que soporta el Banco de Proyectos, sin considerar todo el entorno.

Recomendación(es): Así como se ha establecido la directriz de “Definir lineamientos para ejecutar las pruebas de vulnerabilidades” que deberá ser aplicable a todos los sistemas e infraestructura de la ADR, es necesario establecer y formalizar un proceso para la gestión de las vulnerabilidades técnicas que genere como mínimo la siguiente información: sistemas evaluados, vulnerabilidades críticas identificadas, acciones ejecutadas, monitoreo e indicadores implementados.

Para la construcción de la metodología de análisis de vulnerabilidades se sugiere considerar los lineamientos que propone la CEH Metodología desarrollada por el EC-

Council[10] y que da cumplimiento a los requerimientos establecidos por los estándares ISO 27001:2013. Esta metodología incluye 4 etapas:

- **Etapa 1: Diseño y caracterización de la prueba de análisis de vulnerabilidades**, en la cual se identifica la validación de los objetivos, alcance, asignación de tareas, definición de cronograma y las herramientas a utilizar en las pruebas.

- **Etapa 2: Identificación y clasificación de vulnerabilidades**. Identificación de los riesgos inherentes relacionados con los activos de información, recopilar la mayor cantidad de información acerca del perfil de seguridad de cada uno. Definición del tipo de ataque (activo - pasivo). Identificación de vulnerabilidades

- **Etapa 3: Ataques de intrusión**. Desarrollar un plan de pruebas no intrusivas a los servidores, plan de pruebas de explotación de las vulnerabilidades, e identificación de los falsos positivos. Se deben nombrar los tipos de ataques a realizar (Cracking de password sobre servidores, bases de datos y equipos de protección perimetral, vulnerabilidades técnicas sobre motores de bases de datos, inyección de código malicioso (LDAP, SQL, SSI, Xpath, etc.) a las bases de datos identificadas, entre otros)

- **Etapa 4: Elaborar y presentar el informe** con los resultados del análisis de vulnerabilidades y las recomendaciones a que haya lugar para mejorar la seguridad de la información.

En caso de considerar la contratación de desarrollo externo para la implementación del Acuerdo 10 de 2019 (por el cual se adopta el reglamento para los PIDAR) en el Banco de Proyectos, realizar el análisis de riesgos de seguridad de la información al proveedor previo a la contratación, y con base en el resultado, evaluar la inclusión de una cláusula

10 CEH (Certified Ethical Hacker) es la certificación oficial de hacking ético proporcionada por el Consejo Internacional de Consulta de Comercio Electrónico (EC-Council). El Hacker Ético es la persona que lleva a cabo intentos de intrusión en redes y/o sistemas en los que cuenta con la autorización para realizar las pruebas sobre los sistemas que ataca. Se concentra en como buscar debilidades y/o vulnerabilidades en sistemas usando los mismos conocimientos y herramientas que un hacker pero con fines benévolos.

contractual asociada al desarrollo de pruebas de vulnerabilidad como parte del aseguramiento de la solución en el entorno donde opere; así mismo, deberá incluir la realización de una prueba posterior a la subsanación de las vulnerabilidades previamente identificadas.

Incluir en el documento a elaborar, la alineación y cumplimiento del reporte formal de los incidentes de seguridad de acuerdo con lo establecido en el procedimiento Gestión de Incidentes de Seguridad de la Información (PR-GTI-004) versión 2.

Con base en los resultados de las pruebas de vulnerabilidad que se vayan realizando y gestionando, incluir en el(los) mapa(s) de riesgo(s) de los procesos correspondientes los riesgos asociados a Seguridad de la Información y Ciberseguridad.

Respuesta del Auditado: Aceptado

Justificación: "*Se acepta el hallazgo, dado que la Oficina de Tecnología de la Información de la Agencia de Desarrollo Rural - ADR no tiene documentada una metodología para la realización de pruebas de efectividad para comprobar y medir la eficiencia de los sistemas de información de la ADR. De esta manera, a través de la valoración de diferentes aspectos, permitir e identificar vulnerabilidades y amenazas a las cuales está expuesta la Agencia, así como debilidades y controles implementados. Para efectos de esta auditoría, las pruebas de vulnerabilidad presentadas no contaban con dicha metodología, por lo cual, el análisis técnico entregado por parte del ejecutor del control, no permitiera establecer los impactos internos e identificar falsos positivos*."

Causa(s) identificada(s) por el Responsable de la Unidad Auditada:

- Elaboración de análisis y realización de pruebas de efectividad sin una metodología especifica que pueden causar fallas al sistema de información debido a vulnerabilidades mal evaluadas o no tratadas.

- Ineficientes resultados presentados en las pruebas de vulnerabilidad del Banco de Proyectos.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
De conformidad con el MSPI, se debe contar con una metodología de pruebas de efectividad adoptada por la ADR.	Elaborar la guía metodología de pruebas de efectividad ADR.	Correctiva	Equipo Humano OTI	10-oct-2020	18-dic-2020

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Al analizar el plan de mejoramiento propuesto, se identificaron los siguientes aspectos, los cuales deben ser considerados para su ajuste o complemento:

- "Elaborar la guía metodología de pruebas de efectividad ADR". Al respecto, esta Oficina de Control Interno considera que emprender esta actividad de manera aislada no subsana totalmente el hallazgo presentado en cuanto a la "*Inobservancia del desarrollo de pruebas de vulnerabilidad al Banco de Proyectos y su entorno*", toda vez que, la metodología por sí sola no se constituye como un control que garantice la seguridad, confidencialidad y disponibilidad de la información del Banco de Proyectos, sino que corresponde a un marco metodológico para el desarrollo y ejecución de las pruebas. Con base en lo anterior, la OTI deberá establecer la fecha de programación de las pruebas de vulnerabilidad que incluya todo el entorno del Banco de Proyectos, esto es, hardware, software y sistema operativo.

Como resultado de las pruebas una vez aplicada la metodología a seguir, y con base en la valoración de riesgos, incluir en el(los) mapa(s) de riesgo(s) de los procesos correspondientes los riesgos asociados a Seguridad de la Información y Ciberseguridad.

RESUMEN DE HALLAZGOS:

N°	Título de Hallazgo	Repetitivo	Estado
1	Falta de oportunidad en la instrumentación, formalización y aplicación de lineamientos rectores de la Política de Seguridad y Privacidad de la Información	No	Abierto
2	Inobservancia de las Políticas de Seguridad y Privacidad de la información por usuarios del aplicativo Banco de Proyectos	No	Abierto
3	Incumplimiento de los lineamientos procedimentales establecidos para la creación de cuentas en el Directorio Activo.	No	Abierto
4	Ausencia de lineamientos para la gestión de cuentas de usuario del Directorio Activo a nivel de Eliminación.	No	Abierto
5	Inadecuada gestión y monitoreo de usuarios y roles asignados en el aplicativo Banco de Proyectos	No	Abierto
6	Deficiencia de controles en el proceso de gestión de cambios sobre el sistema y modificaciones directas a datos en producción	No	Abierto
7	Deficiencias en documentación y trazabilidad de los casos registrados en la herramienta de mesa de servicios ARANDA	No	Abierto
8	Ausencia de procedimientos para la gestión de logs y registros de auditoria de actividades realizadas por los usuarios.	No	Abierto
9	Inadecuada gestión y monitoreo de mecanismos de recuperación en caso de contingencia	No	Abierto
10	Ausencia de lineamientos para el monitoreo de capacidad y disponibilidad de la infraestructura tecnológica hardware y software para Banco de Proyectos	No	Abierto
11	Inobservancia del desarrollo de pruebas de vulnerabilidad al Banco de Proyectos y su entorno	No	Abierto

Notas:

- La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Plan Anual de Auditoría, se encuentra limitada por restricciones de tiempo y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.

- La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por la Oficina de Tecnologías de la Información y la Vicepresidencia de Proyectos, a través de solicitudes y consultas realizadas por la Oficina de Control Interno. Nuestro alcance no pretende corroborar la precisión de la información y su origen.

- Es necesario precisar que, las *"Recomendaciones"* propuestas en ningún caso son de obligatoria ejecución por parte de la Entidad, más se incentiva su consideración para los planes de mejoramiento a que haya lugar.

- La respuesta ante las situaciones observadas por la Oficina de Control Interno es discrecional de la Administración de la Agencia de Desarrollo Rural – ADR.

Bogotá D.C., 15 de octubre de 2020.

HÉCTOR FABIO RODRIGUEZ DEVIA
Jefe Oficina de Control Interno

Elaboró: *Luz Paulina Nieto Olarte, Contratista.*

Revisó: *Claudia Patricia Quintero Cometa, Gestor T1.*